AUTORITÉ DES MARCHÉS FINANCIERS

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Le 5 octobre 2022

Version 5.0

Table des matières

1. Préambule

L'adoption et la mise en œuvre de la présente *Politique de sécurité de l'information* (la « Politique ») découlent de l'obligation prévue à l'article 12 de la *Directive gouvernementale sur la sécurité de l'information* (approuvée par le décret no 1514-2021 du 8 décembre 2021), prise en application de l'article 20 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03 (la « Directive gouvernementale »).

Cette Politique remplace la version 4.0 de la *Politique sur la protection et la sécurité de l'information* approuvée le 10 juillet 2017 par la décision n° 2017-PDG-0080 et dont la mise en œuvre a permis de soutenir la mission de l'Autorité des marchés financiers (« l'Autorité »), tout en faisant la promotion d'une culture responsable de la sécurité de l'information et de la protection des renseignements personnels dans le respect du droit à la vie privée.

Les termes utilisés dans la présente Politique ont le sens qui leur est attribué dans le *Lexique commun relatif à la gouvernance des actifs informationnels*, disponible sur l'intranet de l'Autorité.

2. Structure de gouvernance

La Politique est l'une des pièces de gouvernance qui composent le cadre de gouvernance des actifs informationnels de l'Autorité. Elle constitue le fondement normatif en matière de sécurité de l'information et s'appuie sur les principes directeurs énoncés dans la *Politique-cadre de gouvernance des actifs informationnels de l'Autorité* (la « Politique-cadre »), laquelle vise à établir une vision commune de la gouvernance de l'ensemble des actifs informationnels de l'Autorité dans une perspective de cohérence organisationnelle.

La gouvernance en sécurité de l'information de l'Autorité (la « gouvernance SI ») s'inspire de la Directive gouvernementale. Elle vise aussi à rencontrer les attentes énoncées par l'Autorité dans sa Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications. Elle est basée sur le modèle de l'*Institute of Internal Auditors* (« IIA »).

La gouvernance SI adopte donc ce modèle fondé sur les trois lignes qui établit une distinction entre les trois groupes de fonctions impliqués dans la gestion efficace des risques liés à la sécurité de l'information :

1ère ligne :

La gestion des risques est l'apanage du rôle de première ligne. Cette ligne oriente, conduit et exploite les ressources en sécurité de l'information qui sont mises à sa disposition afin de réaliser les objectifs en sécurité de l'Autorité. Cette ligne assure la protection des actifs informationnels de l'Autorité par la mise en œuvre de mesures visant à réduire les risques de toute forme d'atteinte à la disponibilité, la confidentialité ou l'intégrité de l'information, telles des vulnérabilités, menaces ou des cyberattaques, par la mise en place d'actions préventives et correctives permettant de remédier aux déficiences des processus et des contrôles.

Finalement, cette première ligne met en œuvre toute action requise pour la prise en charge d'un événement de sécurité.

La 1ère ligne relève principalement de la Direction principale des technologies de l'information sous la Vice-présidence des services administratifs. Le Responsable de l'accès aux documents et de la protection des renseignements personnels joue aussi un rôle clé au niveau de cette 1ère ligne.

2e ligne :

La 2e ligne est celle des différentes fonctions instituées pour assurer le suivi du contrôle des risques et de la conformité. Nous y retrouvons la fonction de gestion des risques qui facilite et surveille la mise en œuvre de dispositifs efficaces de gestion des risques par les gestionnaires et qui assiste les détenteurs des actifs informationnels dans la définition du niveau cible d'exposition aux risques et la communication d'informations adéquates en matière de risques dans l'ensemble de l'organisation.

Cette ligne vise à « s'assurer » et non « exécuter ». La 2e ligne est notamment assurée par la Vice-présidence stratégie, risques et performance, en collaboration avec la Vice-présidence des services administratifs et la Direction générale des affaires juridiques et du secrétariat.

3e ligne :

La 3e ligne assure l'évaluation systématique et indépendante de tous les processus de gestion des risques, de contrôle et de gouvernance. Elle donne une assurance objective sur la suffisance et l'efficacité de la gouvernance en sécurité de l'information et de la gestion des risques au sein de l'Autorité, incluant les contrôles maintenus par les parties externes.

Pour permettre à l'Autorité de conserver son indépendance, son objectivité, son autorité et sa crédibilité, cette ligne est assumée par le Chef de l'audit interne.

La Politique est soutenue par le *Cadre de gestion de la protection et de la sécurité de l'information* (le « CGPSI ») qui établit les structures fonctionnelles détaillées nécessaires à la gestion et à la mise en œuvre de la sécurité de l'information dans l'organisation en plus de décrire les rôles et responsabilités des intervenants en matière de sécurité de l'information au sein de l'Autorité, en complément de ceux décrits dans la Politique-cadre. Certains titulaires de rôles et responsabilités en sécurité de l'information sont nommés par le Président-directeur général conformément aux exigences gouvernementales.

Des directives, règles, guides et procédures précisant les dispositions à respecter aux fins d'assurer la sécurité de l'information et leurs modalités d'application complètent ce corpus de pièces de gouvernance dont la finalité est de contribuer à la résilience organisationnelle ainsi qu'au maintien de la confiance des diverses parties prenantes envers l'Autorité.

Le tout s'inscrit dans une démarche visant à mettre en œuvre une gouvernance forte et intégrée de la sécurité de l'information qui encadre la gestion, l'utilisation et l'exploitation des actifs informationnels de l'Autorité et prévoit la mise en place des mesures proportionnelles à la valeur de l'information et aux risques encourus afin de prévenir un incident et, en cas d'occurrence, en limiter les impacts.

3. Champ d'application

La Politique s'applique tout au long du cycle de vie de chacun des actifs informationnels détenus par l'Autorité.

Personnes visées :

La Politique s'applique aux utilisateurs, c'est-à-dire tous les membres du personnel de l'Autorité, membres de son conseil d'administration, membres du Conseil consultatif des consommateurs de produits et utilisateurs de services financiers institué par l'article 58.1 de la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1 ainsi que toute personne, entité ou partenaire qui, par un engagement contractuel ou autre, accède, collecte, héberge ou traite de l'information détenue ou générée par l'Autorité à partir de ses locaux ou de n'importe quel autre endroit prévu à ces fins.

Activités visées :

La Politique vise toute activité impliquant la création, la collecte, l'utilisation, le traitement, l'exploitation, la communication, la conservation ou la destruction d'une information ou d'un actif informationnel détenu par l'Autorité, qu'elle soit conduite dans ses locaux ou de n'importe quel autre endroit prévu à ces fins.

4. Objectifs

La Politique affirme l'engagement de l'Autorité à continuer de s'acquitter pleinement de ses obligations en matière de sécurité de l'information, en particulier à l'égard des renseignements personnels, le tout en respect du cadre légal et normatif en vigueur.

Elle vise à établir la stratégie par laquelle l'Autorité entend assurer la sécurité de l'information afin de préserver la disponibilité, l'intégrité et la confidentialité des actifs informationnels qu'elle détient ou qu'elle génère dans le cadre de ses opérations.

Cette stratégie s'articule autour d'axes d'intervention qui sont arrimés à ceux de la *Politique gouvernementale de cybersécurité* publiée par le Secrétariat du Conseil du Trésor en mars 2020 afin d'assurer la mise en œuvre des mesures considérées comme essentielles à la sécurité de l'information nécessaire au soutien des activités de l'Autorité. Ils s'inspirent des meilleures pratiques, notamment des normes ISO27000, des standards du *National Institute of Standards and Technology* (« NIST ») et du *Center for Internet Security* (« CIS »), ainsi que des publications du *SANS Institute*.

5. Axes d'intervention

Une démarche éthique et déontologique, visant notamment la responsabilisation collective et individuelle, soutient le processus de gestion de la sécurité de l'information de l'Autorité. Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être exemplaires, tenir compte des bonnes pratiques reconnues et généralement acceptées à l'échelle nationale et internationale.

L'Autorité assure la sécurité de l'information conformément aux axes d'interventions suivants :

Axe 1 - Se gouverner :

Cet axe d'intervention vise à adopter une gouvernance forte et intégrée reposant sur un cadre légal, administratif et normatif adapté à l'ère du numérique par une vision globale et concertée, renforçant ainsi la confiance des utilisateurs et du public à l'égard de la sécurité de leurs données.

Axe 2 – Se protéger :

La promotion d'une culture positive et responsable de la sécurité de l'information, tant à l'interne que dans l'écosystème dans lequel l'Autorité évolue, notamment auprès de ses partenaires du réseau gouvernemental de cyberdéfense, est clé dans le déploiement de cet axe d'intervention. Il en va de même de l'encouragement au partage et à la mise en commun des connaissances et de l'expertise de même qu'à la mise en œuvre des bonnes pratiques en sécurité de l'information afin que toutes les parties prenantes de l'Autorité soient des utilisateurs numériques avertis.

Il mise sur le développement des personnes, des processus et des technologies afin de tirer profit d'une expertise de pointe. La sensibilisation et la formation des utilisateurs de l'Autorité aux enjeux, mesures et menaces en sécurité de l'information afin de favoriser et d'encourager l'adoption de comportements sécuritaires dans tous les aspects de la sécurité des actifs informationnels est aussi couvert par cet axe.

Axe 3 – Se préparer :

La mise en œuvre des mesures d'atténuation permettant d'assurer la protection et la résilience opérationnelle de l'Autorité lors d'incidents de sécurité, tel que la gestion de crise et la reprise informatique, afin de se prémunir notamment contre les menaces émergentes susceptibles de causer des torts à l'Autorité, au public, aux entreprises ou à ses partenaires constitue le troisième axe d'intervention.

Dans la réalisation de ces axes d'intervention, l'Autorité rend disponibles aux utilisateurs les outils propres à assurer la sécurité de l'information dont elle dispose. Elle met en place les mesures et les contrôles permettant de réduire les risques en sécurité de l'information et veille à leur respect.

6. Respect de la Politique

Tout utilisateur a l'obligation de protéger l'information mise à sa disposition, conformément à la législation applicable et aux codes d'éthique et de déontologie en vigueur à l'Autorité.

Les utilisateurs doivent respecter la présente Politique et les pièces de gouvernance qui en découlent. Ils doivent plus particulièrement consulter les directives applicables afin de connaître les dispositions détaillées d'utilisation des actifs informationnels. Ces directives sont disponibles sur l'intranet de l'Autorité.

Tout utilisateur qui contrevient à la présente Politique, au CGPSI ou à toute directive, règle, guide ou procédure qui en découle, peut faire l'objet d'une mesure administrative, disciplinaire ou autre mesure légale applicable, pouvant aller jusqu'à une fin d'emploi ou à une fin de contrat, selon le cas.

Chaque utilisateur est responsable de signaler à son gestionnaire, ou encore à la Direction de la sécurité de l'information via le processus de déclaration d'incidents de sécurité de l'information, sans tarder, tout événement non conforme à la présente Politique ainsi qu'aux pièces de gouvernance qui s'y rattachent, de même que toute brèche de sécurité suspectée ou mauvaise utilisation des actifs informationnels dont il a connaissance. Il peut aussi effectuer une divulgation anonyme et confidentielle en vertu de la Politique de divulgation d'actes répréhensibles de l'Autorité.

Les gestionnaires, détenteurs des actifs informationnels pertinents à leur secteur d'activités respectif, doivent veiller à l'usage adéquat de ces actifs et s'assurer de leur protection, notamment par la gestion des risques et des vulnérabilités, ainsi que par l'application de mesures visant à les protéger de toute forme d'atteinte, telles des menaces ou des cyberattaques.

Afin d'assurer une saine gestion des ressources ainsi que la protection et la sécurité de l'information, l'Autorité peut effectuer certaines mesures de surveillance par l'intermédiaire des outils de travail mis à la disposition des utilisateurs et des moyens relatifs à la sécurité. Ces mesures de surveillance sont encadrées et effectuées selon les paramètres fixés par le droit applicable et l'ensemble des politiques et directives de l'organisation.

7. Diffusion

Cette Politique est publiée sur l'intranet de l'Autorité.

Pour toute information, question ou demande en lien avec cette Politique, tout membre du personnel peut communiquer avec son gestionnaire ou à la Direction de la sécurité de l'information à l'adresse suivante : securite_information@lautorite.qc.ca.

8. Suivi et Révision

Le suivi et la présentation d'un bilan annuel au Comité de protection et de sécurité de l'information (le « CPSI ») relativement à l'application de la présente Politique sont effectués par le Directeur de la sécurité de l'information.

Une révision complète de cette Politique et de toute pièce de gouvernance qui en découle doit être faite périodiquement par la Direction de la sécurité de l'information pour s'assurer d'être adaptée au cadre légal et normatif applicable ainsi qu'aux bonnes pratiques en sécurité. Cette révision doit minimalement être effectuée tous les cinq ans.

Une mise à jour doit aussi être effectuée lors de changements organisationnels ou stratégiques majeurs ou lorsque jugé opportun par le conseil d'administration, son comité d'audit, le comité de direction ou le CPSI.

9. Approbation et historique des révisions

Version N°	**Recommandation du CGIR au comité d'audit**	**Recommandation du comité d'audit au conseil d'administration**	**Approbation par le conseil d'administration**
5.0	13 juin 2022	4 octobre 2022	5 octobre 2022 Résolution 2022-CA-0027

10. Entrée en vigueur

La Politique entre en vigueur à la date de son approbation par le conseil d'administration le 5 octobre 2022.

CADRE DE GOUVERNANCE DES ACTIFS INFORMATIONNELS DE L'AUTORITÉ DES MARCHÉS FINANCIERS

CA / Comité du CA concerné / CODIR ou CGIR, selon le contexte

Politique-cadre

Gouvernance des actifs informationnels
(Énoncés généraux, principes directeurs, rôles et responsabilités transversaux)
(Date d'entrée en vigueur : 5 octobre 2022)

Lexique commun (Date d'entrée en vigueur : 5 octobre 2022)

CA / Comité du CA concerné / CODIR, CGIR ou CGTI, selon le contexte / CPSI , selon le contexte / Comité sectoriel concerné

Politiques

Gouvernance de l'information
(Date d'entrée en vigueur de la mise à jour: 6 décembre 2023)

Sécurité de l'information
(Date d'entrée en vigueur de la mise à jour: 5 octobre 2022)

Accès à l'information et protection des renseignements personnels
(Date d'entrée en vigueur de la mise à jour: 20 mars 2023)

Gouvernance et gestion des ressources informationnelles (TI)
(2013), Cible d'entrée en vigueur de la mise à jour: 27 mars 2024

CODIR, CGIR ou CGTI, selon le contexte / CPSI, selon le contexte / Comité sectoriel concerné

Cadres de gestion

Information
(Date d'entrée en vigueur: 6 décembre 2023)

Valorisation des données
(Date d'entrée en vigueur: 6 décembre 2023)

Protection et sécurité de l'information
(Date d'entrée en vigueur de la mise à jour: 5 octobre 2022)

CODIR selon le contexte / CPSI ou autre comité institutionnel, selon le contexte / Comité sectoriel concerné

Directives

- Gestion des incidents
- Catégorisation des actifs informationnels
- DMU, infonuagique, Power BI, outils analytiques
- Qualité, collecte, accès, utilisation responsable et éthique des actifs informationnels
- Gestion des métadonnées
- Gestion des investissements en ressources informationnelles et cadre agile (CRAA)

- Calendrier de conservation
- Plan de classification de l'information
- Protection des documents essentiels
- Convention de nommage

- Flux de données
- Utilisation éthique des données (incluant l'IA)

- Sécurité de l'information en mode hybride*
- Utilisation sécuritaire des actifs informationnels*
- Sécurité des systèmes d'information, progiciels et services logiciels***
- Gestion des identités et accès aux actifs informationnels (GIA)
- Gestion des incidents de SI*
- Gestion des risques en SI**
- Accès aux référentiels centraux

Éléments communs

Gestion de l'information

Gouvernance et valorisation des données

Sécurité de l'information
** Approuvé par le CPSI le 16 juin 2022*
*** Approuvé par le CPSI le 17 novembre 2022*
**** Approuvé par le CPSI le 15 décembre 2022*

Gestionnaire de l'unité opérationnelle propriétaire du processus

Règles

- Escalade d'incident de sécurité
- Travail hybride
- Protection des renseignements personnels dans le cadre d'un sondage
- Utilisation des dépôts d'information (ex. répertoires, messageries, applications *SharePoint*, *Teams*, etc.)
- Cycle de vie