



**AUTORITÉ
DES MARCHÉS
FINANCIERS**

**POLITIQUE D'ACCÈS À
L'INFORMATION ET DE
PROTECTION DES
RENSEIGNEMENTS
PERSONNELS**

Le 20 mars 2023

Version 2.0

Table des matières

1. Préambule	3
2. Cadre légal et normatif	3
3. Structure de gouvernance	4
4. Champ d'application	4
Personnes visées :	4
Activités visées :	4
5. Objectifs	5
La transparence, l'accessibilité de l'information et l'exercice des droits de rectification.....	5
La protection des renseignements personnels.....	6
L'utilisation et la communication de l'information	6
La prévention et le signalement de risques.....	6
6. Rôles et responsabilités	7
Membre du personnel :	7
Gestionnaire :	7
7. Respect de la Politique.....	8
8. Diffusion.....	9
9. Suivi et révision	9
10. Approbation et historique des révisions.....	9
11. Entrée en vigueur.....	9

1. Préambule

L'adoption et la mise en œuvre de la présente *Politique sur l'accès à l'information et la protection des renseignements personnels* (la « Politique ») découlent des principes de l'administration publique québécoise qui visent à ce que les organismes publics fassent connaître, en toute transparence, les informations liées à l'exercice de leurs fonctions. Cette diffusion d'information doit cependant être faite en respectant les obligations de confidentialité auxquelles l'Autorité des marchés financiers (l' « Autorité ») est tenue ainsi que le principe de la protection des renseignements personnels, lequel découle du droit à la vie privée.

Cette Politique remplace la version 1.0 de la *Politique sur l'accès à l'information et la protection des renseignements personnels* approuvée le 15 juillet 2009 par la décision n° 2009-PDG-0073 et dont la mise en œuvre a permis de soutenir la mission de l'Autorité, tout en faisant la promotion d'une culture responsable 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. Cadre légal et normatif

À titre d'organisme public, l'Autorité est soumise à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 (la « Loi sur l'accès ») ainsi qu'aux règlements pris en vertu de celle-ci, notamment le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, r.2 (le « Règlement sur la diffusion »).

Cette loi favorise la transparence organisationnelle et prévoit les mesures à suivre par les organismes publics en matière d'accès à l'information et de protection des renseignements personnels. Elle établit également un équilibre entre le droit à l'information et le droit à la vie privée.

Les restrictions aux droits d'accès généraux prévues à la Loi sur l'accès ainsi qu'à certaines dispositions de la loi constitutive de l'Autorité, à savoir la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1 (la « Loi sur l'encadrement »), et des lois qu'elle administre protègent la confidentialité de certains renseignements ou actifs informationnels, détenus par l'Autorité dans l'exercice de ses pouvoirs d'encadrement et d'application de la loi, notamment à la suite d'une inspection ou d'une enquête. Dans la mesure où un dossier devient litigieux, la confidentialité doit aussi être observée sous l'angle du secret professionnel, du privilège relatif aux litiges et des autres privilèges applicables.

Par ailleurs, la présente Politique s'inspire des meilleures pratiques, notamment de la norme ISO 15489 *Information et documentation - Gestion des documents d'activité* et du Manuel du professionnel en AIPRP de l'Association des professionnels en accès à l'information et en protection de la vie privée (« AAPI »).

3. 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 d'accès à l'information et de protection des renseignements personnels (« AIPRP »). Elle 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.

Cette vision commune est soutenue par la présente Politique qui contribue à mettre en œuvre une gouvernance forte et intégrée en matière de gestion, d'utilisation et d'exploitation des actifs informationnels de l'Autorité et prévoit la mise en place des mesures de protection 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.

La Politique est soutenue par le *Cadre de gestion de la protection et de la sécurité de l'information* (le « CGPSI ») qui soutient également la *Politique de sécurité de l'information* dont les objectifs convergent vers ceux de la présente Politique afin d'assurer le respect des obligations de l'Autorité en matière d'AIPRP. Le CGPSI établit les structures fonctionnelles détaillées nécessaires à la gestion et à la mise en œuvre de la protection et 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.

4. 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 ainsi que toute personne, incluant les membres externes des comités consultatifs constitués par l'Autorité de même que toute entité ou tout 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'organisation, l'utilisation, le transfert d'un support à un autre, le traitement, l'exploitation, la circulation à l'interne, la communication, la transmission, la diffusion, la publication, 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.

5. Objectifs

La Politique affirme l'engagement de l'Autorité à continuer de s'acquitter pleinement de ses obligations en matière d'AIPRP, le tout en respect du cadre légal et normatif en vigueur.

Cette Politique a pour but d'établir un encadrement à la fois clair et efficace pour l'ensemble des activités visées par la Politique, en cohésion avec les principes de saine gouvernance et gestion de l'information.

Plus spécifiquement, la Politique vise à maintenir et renforcer la culture d'accès à l'information et à la protection des renseignements personnels au sein de l'Autorité et à assurer un traitement adéquat de l'information vers l'atteinte des objectifs suivants :

- créer un équilibre entre le droit au respect de la vie privée, l'exercice des droits d'accès et de rectification et la transparence organisationnelle;
- assurer la réalisation conforme et efficace des obligations de l'Autorité en matière d'AIPRP;
- assurer la compréhension par tous les membres du personnel des enjeux et principes fondamentaux en matière d'AIPRP; et
- adapter toute mesure d'application de la Politique aux changements technologiques et organisationnels.

Ces objectifs découlent des énoncés suivants, lesquels constituent les fondements de la Politique :

La transparence, l'accessibilité de l'information et l'exercice des droits de rectification

L'Autorité, en tant qu'organisme public, fait preuve de transparence et diffuse sur son site Internet les documents ou renseignements accessibles en vertu de la Loi sur l'accès qui sont identifiés dans le Règlement sur la diffusion. Elle diffuse aussi de l'information concernant les règles encadrant sa gouvernance à l'égard des renseignements personnels ainsi que ses politiques et pratiques encadrant une telle gouvernance, le tout conformément à la Loi sur l'accès et au Règlement sur la diffusion. Elle facilite l'exercice du droit d'accès, favorise la publication d'information notamment par l'Internet et divers réseaux sociaux ainsi qu'elle encourage la divulgation volontaire d'information ou la diffusion active de l'information par une unité administrative.

Les membres du personnel donnent accès à l'intégralité d'un dossier lorsque le Responsable de l'accès aux documents et de la protection des renseignements personnels (le « RADPRP ») en fait la demande dans l'exercice de ses fonctions.

Plus particulièrement, sous réserve de la loi, un document ou renseignement détenu par l'Autorité est accessible sur demande écrite ou verbale, sans égard au motif qui anime le demandeur. Un demandeur a également accès aux renseignements personnels le concernant et il peut demander, au besoin, une rectification de ceux-ci.

Toutefois, l'Autorité peut restreindre ou refuser l'accès à un document ou à un renseignement qu'elle détient, notamment lorsqu'une disposition de la Loi sur l'accès, de la Loi sur l'encadrement ou des lois administrées par l'Autorité le prévoit.

La protection des renseignements personnels

L'Autorité ne détient que le renseignement personnel nécessaire à l'exercice de ses attributions. Elle s'assure que le renseignement conservé est exact, complet, sécurisé et mis à jour. Elle en assure l'intégrité et, à moins que la Loi sur l'accès, la Loi sur l'encadrement, les lois qu'elle administre ou toute autre loi applicable ne lui confèrent un caractère public, sa confidentialité.

L'Autorité prend les mesures de sécurité propres à assurer la protection des renseignements personnels créés, collectés, utilisés, communiqués et conservés et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support et ce, jusqu'à leur destruction en conformité avec le calendrier de conservation de l'Autorité.

L'utilisation et la communication de l'information

- Utilisation

Un renseignement personnel ne peut être utilisé au sein de l'Autorité qu'aux fins pour lesquelles il a été recueilli.

Il ne peut être utilisé à d'autres fins, sauf avec le consentement de la personne concernée ou exceptions prévues par la Loi sur l'accès (1° à des fins compatibles avec celles pour lesquelles il a été recueilli (ayant un lien direct, prévisible et pertinent avec l'utilisation primaire), 2° au bénéfice manifeste de la personne concernée ou 3° nécessaire à l'application d'une loi au Québec).

Au sens de la Loi sur l'accès, une communication entre membres du personnel de différentes unités administratives d'une organisation est une forme d'utilisation de l'information. La présente Politique vise donc toutes les formes d'utilisation, y compris la circulation à l'interne.

Un renseignement personnel ne peut circuler à l'interne ou être autrement accessible, sans le consentement de la personne concernée, que lorsqu'il est nécessaire aux fonctions du membre du personnel qui y a accès.

- Communication

La notion de communication réfère à une communication à l'externe.

L'Autorité ne peut communiquer un renseignement personnel sans le consentement de la personne concernée, sauf dans les cas prévus par la loi.

De plus, le membre du personnel ne doit communiquer ou permettre que soit communiqué de l'information que s'il y est autorisé par l'Autorité et que le cadre légal et normatif le permet selon la nature des renseignements concernés.

La prévention et le signalement de risques

L'Autorité anticipe et évalue les principaux risques susceptibles de survenir en matière de protection des renseignements personnels ou autres renseignements confidentiels, le tout conformément aux meilleures pratiques. La collaboration des membres du personnel est essentielle afin de prévenir les risques ou incidents susceptibles d'affecter la confidentialité ou l'intégrité de l'information détenue.

6. Rôles et responsabilités

Les principaux rôles et responsabilités en matière d'AIPRP sont définis dans la Politique-cadre, notamment ceux du conseil d'administration de l'Autorité, de son Président-directeur général, du Chef de l'Audit interne, du Secrétaire et directeur général des affaires juridiques (le « DGSAJ »), du RADPRP désigné conformément à la Loi sur l'accès et du Responsable de la gouvernance et de la gestion de l'information (le « RGGI »).

Le CGPSI prévoit la mise en place du Comité de protection et de sécurité de l'information (le « CPSI ») conformément à la Loi sur l'accès et au Règlement sur la diffusion afin de soutenir l'Autorité dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de cette loi, notamment. Le mandat de ce comité est d'appuyer le Président-directeur général et le Comité de gestion intégré des risques (le « CGIR ») dans les orientations stratégiques, les plans et pratiques en matière de protection et de sécurité de l'information.

Le CGPSI décrit aussi les rôles et les responsabilités dévolus aux membres du personnel qui doivent plus spécifiquement contribuer au développement, à la mise en œuvre et à l'évolution d'une véritable culture de l'accès à l'information et de la protection des renseignements personnels.

En outre, tous les utilisateurs des actifs informationnels détenus par l'Autorité ont des responsabilités en matière d'AIPRP.

Membr e du personnel :

Le membre du personnel joue un rôle de première importance en matière d'accès en appliquant quotidiennement les mesures qui découlent de la Politique afin de permettre à l'Autorité de respecter le cadre légal et normatif applicable. Tout membre du personnel :

- assiste et appuie le RADPRP ou toute autre personne à qui une responsabilité est attribuée en vertu de la Politique;
- participe activement à la formation auquel il est convoqué afin d'améliorer ses connaissances en matière d'accès et de protection des renseignements personnels;
- contribue à l'amélioration des pratiques de l'Autorité en matière d'accès en formulant au RADPRP tout commentaire susceptible de remédier à une lacune ou une vulnérabilité entraînant un risque potentiel à l'égard de renseignements personnels ou confidentiels.

Gestionnaire :

Le membre du personnel qui est le gestionnaire d'une unité administrative :

- s'assure de l'application, au sein de son unité administrative, de la Loi sur l'accès et de la Politique, du CGPSI et de tout autre texte ou mesure qui en découle ainsi que des dispositions de la Loi sur l'encadrement et des lois administrées par l'Autorité en matière d'accès et de protection des renseignements personnels;
- collabore avec le RADPRP à la réalisation de tout mandat relié à l'accès et à la protection des renseignements personnels;

- agit à titre de répondant de 1ère ligne en accès et en protection des renseignements personnels et, à ce titre, appuie le personnel dans la résolution d'une problématique ou d'un enjeu lié;
- répond à toute demande formulée par le RADPRP ou le CPSI;
- lorsque nécessaire, est invité à participer à une séance du CPSI et assure la liaison entre son unité administrative et le RADPRP.

7. 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* disponible sur l'intranet 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.

8. 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 le RADPRP à l'adresse suivante : secretariat@lautorite.qc.ca.

9. Suivi et révision

Le suivi et la présentation d'un bilan annuel au CGIR et au conseil d'administration relativement à l'application de la présente Politique sont effectués par le DGSAJ.

Une révision complète de cette Politique et de toute pièce de gouvernance qui en découle doit être faite périodiquement par le RADPRP pour s'assurer d'être adaptée au cadre légal et normatif applicable ainsi qu'aux bonnes pratiques en accès à l'information et en protection des renseignements personnels. 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 de gouvernance et d'éthique, le comité de direction ou le CPSI.

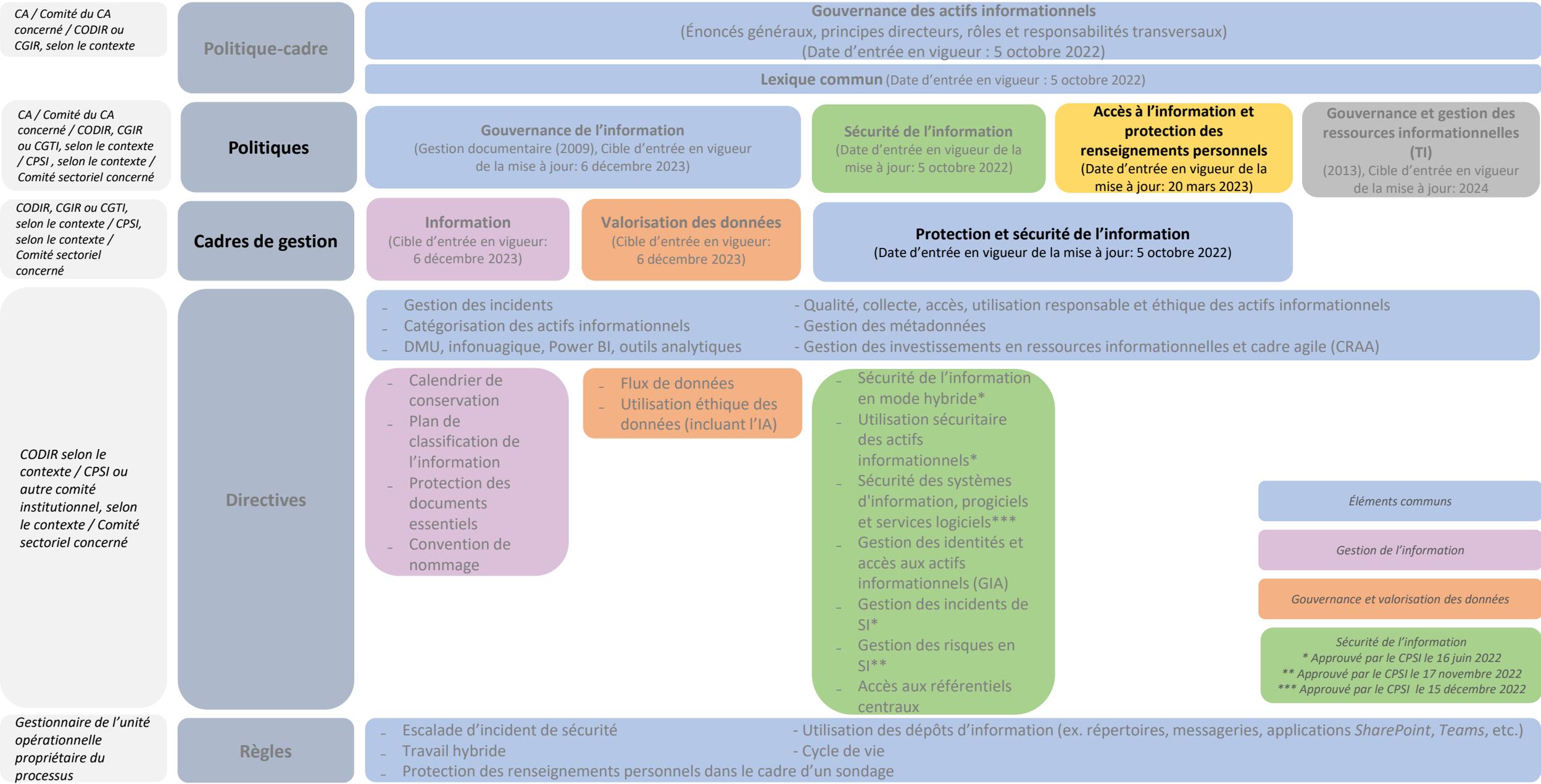
10. Approbation et historique des révisions

Version N°	Recommandations du DGSAJ au CGIR	Recommandation au comité de gouvernance et d'éthique	Recommandation du comité de gouvernance et d'éthique au conseil d'administration	Approbation par le conseil d'administration
2.0	24 novembre 2022 et 15 février 2023	1 ^{er} mars 2023	1 ^{er} mars 2023	20 mars 2023 Résolution 2023-CA-0010

11. Entrée en vigueur

La Politique entre en vigueur à la date de son approbation par le conseil d'administration le 20 mars 2023.

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



- 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