G-11 : POLITIQUE DE SÉCURITÉ ET DE PROTECTION DE l'INFORMATION

Adoptée le 2 juin 2023

TABLE DES MATIÈRES

Politique		Numéro	Date d'entrée en vigueur
Politique de sécurité et de protection de l'information		**G-11**	5 juin 2023
Adoptée par	**Résolution**	**Date**	**Révisée le**
Conseil d'administration	CA-2023-51	2 juin 2023	

CONTEXTE

L'A.P.E.S. recueille et utilise, dans le cadre de ses fonctions, diverses informations dont certaines relatives à ses membres. Ces informations peuvent être de nature publique ou privée et sont incluses dans divers documents auxquels ses représentants ont accès. L'A.P.E.S. est à cet égard soucieuse de la sécurité et de la protection des données qu'elle recueille, notamment auprès de ses membres, de ses partenaires et de ses fournisseurs. À cet effet, elle met à en place des mesures visant à s'assurer que l'information détenue est utilisée pour les fins auxquelles elle est destinée et que sa collecte, son utilisation et sa destruction sont conformes aux normes, lois et règlements en vigueur.

L'objet de cette politique est de permettre à l'Association d'accomplir sa mission, en respectant les lois et en réduisant les risques, tout en protégeant les données confidentielles qu'elle a recueillies et dont elle a la responsabilité. Ces données sont accessibles dans des formats numériques et non numériques. En cas de divulgation ou d'utilisation non autorisée de celles-ci, des conséquences significatives peuvent survenir sur les éléments suivants :

- La vie, la santé ou le bien-être des personnes propriétaires de ces données ;
- L'atteinte à la protection des renseignements personnels et à la vie privée ;
- La prestation de services aux membres ;
- L'image de l'Association et de la profession de pharmacien d'établissement.

Ainsi, cette politique réfère à des mécanismes qui permettent la gestion des risques, des incidents et de l'accès à l'information.

1. CHAMPS D'APPLICATION

1.1. La présente politique concerne toutes les informations confidentielles que l'Association détient et s'applique aux personnes suivantes :

- Membres du conseil d'administration et directrice générale de l'A.P.E.S. ;
- Employés de l'A.P.E.S., stagiaires et pharmaciens libérés professionnellement pour œuvrer au sein de l'A.P.E.S. ;
- Membres de l'A.P.E.S., peu importe la catégorie de membres, et non membres cotisants ;
- Sous-traitants, fournisseurs et autres personnes travaillant ou œuvrant pour le compte de l'A.P.E.S. ;
- Toute personne physique ou morale dûment autorisée qui a accès ou qui utilise des informations confidentielles détenues par l'Association.

La présente politique doit être portée à la connaissance des personnes visées afin qu'elle trouve pleinement application.

1.2. Les informations publiques ne sont pas visées par la présente politique.

1.3. Les personnes visées par la présente politique doivent :

- Respecter la *Politique de sécurité et de protection de l'information*, les procédures et les mesures de protection mises en place en ce qui a trait à l'accès et à l'utilisation des technologies de l'information mises à leur disposition;
- Utiliser l'information détenue par l'A.P.E.S. à laquelle elles accèdent uniquement lorsque celle-ci est requise pour l'exercice de leurs fonctions, en se limitant aux fins auxquelles elle est destinée ;
- S'assurer que les données sont recueillies, conservées et détruites de manière appropriée, en conformité avec la présente politique, ainsi qu'avec la politique RH-13 *Sécurité et protection de l'information*, le cas échéant ;
- Choisir un mot de passe robuste (voir notamment à ce propos le site web du gouvernement du Canada : https://www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032) afin d'accéder aux systèmes d'information de l'A.P.E.S. et s'assurer de ne pas partager leurs mots de passe et leurs codes d'accès personnels confidentiels ;

- Se conformer aux exigences légales existantes en matière de sécurité et de protection des données et de protection des renseignements personnels ;

- Respecter les mesures de sécurité mises en place sur tous les équipements, systèmes d'information, applications ou tout autre environnement donnant accès à des données détenues par l'A.P.E.S. ;

- Signaler immédiatement au responsable de la protection des renseignements personnels nommé en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* toute situation dont elles ont connaissance pouvant constituer une violation de la présente politique ou des lois et règlements en vigueur selon la procédure prévue.

1.4 Toute personne qui contrevient aux règles en vigueur dans la présente politique peut se voir refuser l'accès aux ressources informationnelles et aux technologies de l'information de l'Association.

2. PRINCIPES DIRECTEURS

2.1. L'A.P.E.S. reconnaît l'importance de la présente politique et en assure l'application.

2.2. L'A.P.E.S. considère que le traitement des informations confidentielles doit recevoir une attention particulière.

2.3. L'A.P.E.S. est responsable de la sécurité et de la protection des renseignements personnels qu'elle détient tout au long de leur cycle de vie, soit au moment de leur obtention, lors de leur utilisation et de leur conservation ainsi qu'au moment de leur destruction, conformément à la loi.

2.4. À cet effet, l'A.P.E.S. recueille uniquement les renseignements personnels nécessaires afin de remplir sa mission.

2.5. L'A.P.E.S. en limite l'accès et l'utilisation aux personnes autorisées à les recevoir au sein de l'Association lorsque cela est nécessaire à l'exercice de leurs fonctions.

2.6. L'A.P.E.S. s'assure de détenir l'autorisation de la personne concernée avant de communiquer un renseignement personnel la concernant, excepté dans la mesure prévue par la loi.

2.7. La destruction de tout renseignement personnel se fait de manière sécuritaire en fonction du calendrier de conservation de l'Association.

2.8. L'A.P.E.S. reconnaît que l'environnement technologique est en constante évolution et qu'il est interconnecté avec des systèmes extérieurs à l'Association.

3. DÉFINITIONS

3.1 Les termes suivants se définissent comme suit pour l'application de la présente politique :

Cycle de vie de l'information : L'ensemble des étapes que franchit l'information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le Plan de classement-Conservation de l'Association.

Document : Un document est un ensemble d'informations délimitées et structurées de façon tangible ou logique sur un support adapté, intelligible sous forme de mots, de sons ou d'images.

Incident de confidentialité : Les événements suivants constituent des incidents de confidentialité :

- L'accès non autorisé par une loi ou par la présente politique à un renseignement personnel ;
- L'utilisation non autorisée par une loi ou par la présente politique d'un renseignement personnel ;
- La communication non autorisée par une loi ou par la présente politique d'un renseignement personnel ;
- La perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Information : Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Information confidentielle : Information accessible uniquement aux personnes ou entités désignées et autorisées, et ne pouvant être divulguée qu'à celles-ci. À ce titre, tout renseignement personnel est une information confidentielle.

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 et de protection de l'information*.

Responsable de la protection des renseignements personnels : L'A.P.E.S. désigne un responsable de la protection des renseignements personnels. À cet effet, l'Association s'assure que cette information, ainsi que les coordonnées utiles et les rôle et responsabilités de celui-ci, sont publiées dans la section publique de son site Web.

Sécurité de l'information : Protection de l'information et des systèmes d'information contre les risques et les incidents.

4. GESTION DES RISQUES

4.1 Le conseil d'administration de l'A.P.E.S. adopte et maintient en vigueur une politique de ressources humaines (RH-13 *Sécurité et protection de l'information*) afin de préciser les modalités entourant la collecte, l'utilisation et la destruction des informations par les employés, les stagiaires, les pharmaciens libérés professionnellement de leur établissement et les travailleurs autonomes qui œuvrent pour le compte de l'Association. Cette politique vise à assurer le maintien de la sécurité et de la confidentialité de l'information dès son obtention par l'A.P.E.S. et tout au long de son cycle de vie.

4.2 En ce qui concerne les systèmes d'information utilisés par l'Association, le degré de risques, eu égard aux caractéristiques des informations détenues par l'A.P.E.S., guide l'acquisition, le développement, l'évolution, les mises à jour et l'utilisation de ceux-ci.

4.3 Ainsi, l'A.P.E.S. s'assure que les informations confidentielles sont conservées selon les meilleures pratiques en matière de sécurité et qu'un protocole de communication sécurisé est utilisé pour leur transmission.

4.4 L'A.P.E.S. s'assure aussi que des sauvegardes quotidiennes des documents numériques détenus sont faites et qu'elles sont dupliquées sur un serveur distant situé dans un autre lieu physique.

4.5. Également, l'A.P.E.S. met en place les mesures appropriées et s'assure qu'elles sont mises à jour régulièrement afin de réduire les risques de vol ou de perte des informations détenues.

4.6 L'A.P.E.S. s'engage finalement à procéder, aux moments opportuns, à la mise en place de mesures complémentaires conformes aux normes de l'industrie afin de réduire les risques associés à l'utilisation des informations détenues.

5. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

5.1. L'A.P.E.S. met en place des mesures de sécurité visant à limiter l'occurrence d'incidents liés à l'information confidentielle qu'elle détient et s'assure de gérer adéquatement ces incidents afin d'en minimiser les conséquences, le tout conformément à la Loi sur la protection des renseignements personnels dans le secteur privé.

5.2. Ainsi, si l'Association a des raisons de croire qu'un incident de confidentialité visant un renseignement personnel est survenu, elle prend toutes les mesures raisonnables afin de diminuer les risques qu'un préjudice soit causé et d'éviter qu'un nouvel incident de même nature se reproduise. Les mesures raisonnables à mettre en place dépendent de la situation et sont déterminées au fur et à mesure que les circonstances et les effets de l'incident se précisent.

5.3. Pour tout incident de confidentialité, le responsable de la protection des renseignements personnels évalue la gravité du risque de préjudice pour toutes les personnes impliquées en fonction de la sensibilité des renseignements visés, des conséquences appréhendées de leur utilisation et de la probabilité qu'ils soient utilisés à des fins préjudiciables.

5.4. Advenant que l'analyse fasse ressortir un risque de préjudice sérieux, le responsable de la protection des renseignements personnels avise avec diligence la Commission d'accès à l'information ainsi que les personnes concernées de l'incident.

5.5. Le responsable de la protection des renseignements personnels peut communiquer les renseignements personnels nécessaires à toute personne physique ou morale susceptible de diminuer le risque de préjudice sérieux, sans le consentement de la ou des personnes concernées. Cette communication doit toutefois être enregistrée au registre des communications des renseignements personnels.

5.6. L'A.P.E.S. doit tenir un registre des incidents de confidentialité. L'ensemble des incidents de confidentialité concernant un renseignement personnel qu'elle détient, même ceux ne présentant pas de risques sérieux de préjudice, doit y être colligé.

6. ACCÈS À L'INFORMATION

6.1. À moins d'exceptions prévues par la loi, seule la personne concernée peut demander d'accéder à son dossier.

6.2. Toute demande d'accès doit être faite par écrit auprès du responsable de la protection des renseignements personnels.

6.3. L'A.P.E.S. doit répondre à la demande d'accès dans les 30 jours civils de la réception de celle-ci.

6.4. Toute demande de rectification doit être faite par écrit auprès du responsable de la protection des renseignements personnels.

6.5. L'A.P.E.S. conserve les dossiers personnels tant et aussi longtemps que l'objet pour lequel il a été constitué n'est pas terminé.

7. ENTRÉE EN VIGUEUR DE LA POLITIQUE

La présente politique entre en vigueur le jour suivant le jour de son adoption par le conseil d'administration.