Ordre des
hygiénistes dentaires
du Québec

POLITIQUE DE GESTION ET PROTECTION DE L'ACTIF INFORMATIONNEL

RÉFÉRENCE :	**Politique de gestion et protection de l'actif informationnel**
TYPE DE POLITIQUE :	**Gouvernance**
RÉFÉRENCES JURIDIQUES :	- Code des professions - Loi concernant le cadre juridique des technologies de l'information C-1.1 - Loi concernant le cadre juridique des technologies de l'information - Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (ci-après la « LAI ») A-2.1 - Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels - Loi sur la protection des renseignements personnels dans le secteur privé (ci-après la « LP ») P-39.1 - Loi sur la protection des renseignements personnels dans le secteur privé - Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25) - Code civil du Québec, notamment quant aux articles 36 et 37 - Charte des droits et libertés de la personne du Québec, notamment quant aux articles 5 et 9 - La Loi canadienne antipourriel (L.C. 2010, Chapitre 23) - La Loi sur les archives (LRQ, chapitre A-21.1) - La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03) - Règlement sur l'anonymisation des renseignements personnels

ADOPTÉE LE :	**11 novembre 2022**
RÉSOLUTION :	**CA-2223-75**
EN VIGUEUR LE :	**11 novembre 2022**
RÉVISIONS :	**17 novembre 2023 (CA-2324-54)** **15 novembre 2024 (CA-2425-59)**
NOTE :	

Table des matières

PRÉAMBULE

Dans le cadre de sa mission, l'Ordre des hygiénistes dentaires du Québec (ci-après l'« Ordre ») recueille, utilise, traite, communique, conserve et détruit de l'information de nature sensible, personnelle et confidentielle, dont des renseignements personnels. Cette information se trouve sur différents supports (numérique ou papier).

En plus des obligations légales qui incombent aux entreprises et aux organismes publics, dont l'Ordre, quant à la protection des renseignements personnels qu'ils collectent ou détiennent, la sécurité de son actif informationnel constitue une préoccupation importante pour l'Ordre en raison des enjeux contemporains liés notamment aux risques cybernétiques.

Ainsi, la présente Politique a pour but d'établir un encadrement général en vue d'assurer une gestion diligente par l'Ordre de son actif informationnel, et ce, notamment par la mise en place de mesures adéquates visant à en préserver sa sécurité, sa disponibilité, son intégrité et sa confidentialité.

La présente Politique a ainsi pour objectifs :

- La clarification des rôles et responsabilités quant à la gestion et la protection de l'actif informationnel, dont la protection des renseignements personnels ;

- L'implantation, l'uniformisation, l'adoption et l'application en continu de mesures de contrôle administratives, technologiques et physiques de l'actif informationnel, et ce, tout au long de son cycle de vie (collecte, utilisation, communication, conservation et destruction) ;

- L'établissement de principes directeurs en matière de gestion des risques, gestion des accès et gestion des incidents de sécurité propres à l'actif informationnel et aux renseignements personnels.

Outre que pour assurer la conformité de l'Ordre quant à ses obligations légales, le respect de cette Politique permet une saine gestion de l'actif informationnel par l'Ordre, ce qui contribue à protéger les renseignements personnels et minimiser les risques liés à un potentiel incident de sécurité.

PORTÉE

La Politique de gestion et protection de l'actif informationnel s'applique :

- À tous les employés de l'Ordre, ainsi qu'aux tiers opérant pour l'Ordre, que ce soient des fournisseurs, dirigeants, administrateurs, consultants, partenaires d'affaires, membres des comités de l'Ordre ou toute entité mandataire (ci-après les « **Intervenants** ») ;

- À tout **actif informationnel** de l'Ordre ;

- À toutes les activités impliquant la collecte, l'utilisation, la communication, la conservation et la destruction de tout actif informationnel, et ce, sans égard au lieu où ces activités sont effectuées.

DÉFINITIONS

La Politique repose sur les concepts ci-après définis :

- **Actif informationnel (AI) :** Actif composé d'information ou soutenant celle-ci, y compris toute information obtenue, détenue ou communiquée par l'Ordre ou lui appartenant, mais détenu par un tiers, ainsi que les supports tangibles ou intangibles (p. ex. : papier, matériel, logiciel, réseau, etc.) permettant son traitement, sa communication ou sa conservation aux fins de l'utilisation pour lequel il a été obtenu. L'actif informationnel comprend les renseignements personnels.

- **Comité d'accès à l'information et à la protection des renseignements personnels (CAIPRP**) : Comité chargé de soutenir l'Ordre dans l'exercice de ses responsabilités et dans l'exécution de ses obligations légales en matière d'accès à l'information et de protection des renseignements personnels.

- **Confidentialité** : Propriété d'un renseignement de n'être accessible qu'aux personnes désignées et autorisées.

- **Cycle de vie d'un actif informationnel** : Ensemble des étapes franchies par une information ou un renseignement personnel, de sa création ou collecte jusqu'à sa conservation ou sa destruction (collecte, utilisation, enregistrement, consultation, communication, conservation et destruction), et ce, selon le plan de classification et de conservation de l'Ordre.

- **Incident de confidentialité (IC) :** Accès, utilisation ou communication verbale ou écrite non autorisés par la loi d'un renseignement personnel ou la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

  Exemples d'incident de confidentialité :
  - Envoi d'un courriel contenant des renseignements personnels au mauvais destinataire;
  - Un membre du personnel qui consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions en outrepassant les droits d'accès qui lui ont été consentis;
  - Un membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;
  - Une communication verbale de renseignements personnels par l'employeur faite par erreur à la mauvaise personne;
  - Une personne qui perd ou se fait voler des documents contenant des renseignements personnels;
  - Une personne qui s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

- **Incident de sécurité (IS)** : Incident affectant la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel de l'Ordre. Tout incident de confidentialité est considéré comme un incident de sécurité, mais pas nécessairement l'inverse. Un incident de sécurité peut impliquer un actif informationnel de l'Ordre (p. ex. : un énoncé de position confidentiel), sans toutefois que cet actif ne contienne des renseignements personnels. Dans un tel cas, il ne s'agit pas d'un incident de confidentialité au sens de la *Loi sur l'accès aux documents des organismes publics et à la protection des renseignements personnels* (LAI) et de la *Loi sur la protection des renseignements personnels dans le secteur privé* (LP).

Exemples d'incident de sécurité:

- Cyberattaque à l'encontre de la base de données des membres;
- Sinistre aux bureaux de l'Ordre mettant en péril l'intégrité d'actifs informationnels en format papier.

- **Registre des incidents** : registre tenu par le responsable des renseignements personnels en vertu de la Loi modernisant la protection des renseignements personnels.

- **Renseignement personnel (RP) :** Renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Il est confidentiel, à moins que la loi ne lui octroie un caractère public (certains renseignements ont un caractère public en vertu des articles 108.6 à 108.8 du *Code des professions*, comme les renseignements contenus à l'article 46.1 du *Code des professions* lorsqu'ils concernent une personne identifiée).

- **Intervenants** : Désigne notamment les employés, membres du personnel, dirigeants, administrateurs, consultants, fournisseurs, partenaires d'affaires, membres des comités de l'Ordre ou toute entité mandataire.

PRINCIPES DIRECTEURS

Importance et valeur de l'actif informationnel

L'Ordre et ses employés reconnaissent l'importance et la valeur de tout actif informationnel qu'il détient et en comprennent l'importance de le protéger pour en assurer sa sécurité, sa disponibilité, son intégrité et sa confidentialité.

Pour assurer une saine gestion et une protection adéquate de l'actif informationnel, il importe de le prendre en considération dans tous les aspects organisationnels de l'Ordre par une approche globale et intégrée principalement à :

- La gestion des risques ;
- La gestion des accès ;
- La gestion des renseignements personnels et
- La gestion des incidents de sécurité.

Cycle de vie de l'actif informationnel

Cette Politique et les procédures, lignes directrices ou guides qui peuvent en découler couvrent tout le cycle de vie de l'actif informationnel, et ce, indépendamment du support qu'il revêt.

Sécurité de l'information

En cohésion avec la Politique de gestion documentaire de l'Ordre, des mesures appropriées doivent être prises pour assurer la sécurité de l'actif informationnel de l'Ordre, dont les renseignements personnels, et ce, à toute étape de son cycle de vie, notamment pour en assurer sa protection, son intégrité et sa confidentialité.

Intégration à la culture organisationnelle

Afin de faciliter la sensibilisation et la formation des employés, des documents explicatifs tels qu'un guide d'application sont développés et diffusés. Des activités de sensibilisation (p. ex. séances d'information ou de formation) sont dispensées à l'ensemble des employés de façon récurrente. De telles séances sont également intégrées au plan d'intégration de tout nouvel employé, membre de comité ou administrateur. Outre la présente politique, de la documentation est produite et mise à la disposition du personnel (p. ex. : aide-mémoire, etc.).

1.00 RÔLES ET RESPONSABILITÉS

Toute personne ayant accès à un actif informationnel de l'Ordre assume des responsabilités en matière de sécurité et en est redevable. Tous les intervenants de l'Ordre exercent ainsi des responsabilités en matière de gestion et de protection de l'actif informationnel.

1.01 CONSEIL D'ADMINISTRATION

Le Conseil d'administration est chargé de la surveillance générale de l'Ordre, ainsi que de l'encadrement et de la supervision de la conduite des affaires de l'Ordre. Il veille à l'application du Code des professions, ainsi que des Règlements de l'Ordre et voit à l'intégrité des règles de contrôle interne.
À cet effet, il est notamment propriétaire de la Politique de gestion et protection de l'actif informationnel.

Il est aussi responsable de :

- Adopter la Politique de gestion et protection de l'actif informationnel, ainsi que les orientations stratégiques en la matière ;
- Adopter le budget pour la mise en place de mesures de gestion ou de protection ;
- Adopter le plan de gestion des risques et en assurer le suivi périodique ;
- Contribuer à la prise de décisions en lien avec la gestion de crise et en définir les orientations stratégiques, lorsque requis (enjeux réputationnels, etc.).

Pour plus d'information, consultez la page du site web de l'Ordre portant sur le Conseil d'administration.

1.02 DIRECTION GÉNÉRALE

La direction générale assure l'administration générale et courante des affaires de l'Ordre (p. ex. : la gestion des ressources humaines, matérielles et financières). À cet effet, elle met en application les règles de gouvernance, politiques ou procédures au sein de l'Ordre.

1.03 RESPONSABLE DE L'ACCÈS À L'INFORMATION ET À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La personne responsable de la protection des renseignements personnels (RPRP) est la plus haute autorité de l'entreprise, soit le ou la président(e) de l'Ordre. La personne qui occupe ce poste peut toutefois déléguer en tout ou en partie cette fonction. La personne occupant le poste de président de l'Ordre a délégué cette fonction à la personne occupant le poste de directeur(trice) des affaires juridiques et secrétaire adjoint(e). Le ou la Syndic(que) remplit la fonction de RPRP à l'égard des documents et renseignements qu'il ou elle obtient ou détient de même que ceux qu'il ou elle communique au sein de l'Ordre.

Le ou la président(e) de l'Ordre désigne à titre de responsable substitut le ou la directeur(trice) général(e) et le ou la Syndic (que) désigne à titre de responsable substitut le ou la syndic(que) adjoint(e).

Au sein de l'Ordre, la fonction de responsable de la protection des renseignements personnels a été délégué au Directeur ou à la directrice des affaires juridiques et secrétaire adjoint.e.

La personne RPRP a pour mandat d'exercer les fonctions que la LAI et la LP lui confèrent. Elle veille ainsi

à assurer le respect et la mise en œuvre des politiques et pratiques encadrant la gouvernance de l'Ordre à l'égard des renseignements personnels qu'il détient, et ce, afin de répondre aux exigences découlant du cadre juridique applicable en la matière. Il est, avec le Comité d'accès à l'information et à la protection des renseignements personnels (CAIPRP), principalement responsable de :

- Voir à la conformité des consentements recueillis par l'Ordre et assister la personne concernée pour assurer sa compréhension de la portée du consentement qui est demandé (art. 53.1 LAI/14 LP) ;
- Enregistrer la communication de RP à toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux causé par un incident de confidentialité (art. 63.6 LAI/3.5 LP) ;
- Être consulté.e et participer à l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité (art. 63.9 LAI et art. 3.7 LP) ;
- Recevoir les demandes d'accès et de rectification des renseignements personnels et y répondre, prêter assistance au demandeur afin d'identifier les renseignements recherchés et l'aider à comprendre la décision rendue à cet égard (art. 94 et Ss. LAI, art. 30 et 34 LP) ;
- Recevoir et traiter toute plainte relative à la protection des renseignements personnels ;
- Participer, avec le CAIPRP, à l'établissement et à la mise en œuvre des politiques et des pratiques encadrant la gouvernance de l'ordre à l'égard des renseignements personnels et propres à assurer la protection de ces derniers (art. 63.3 LAI et art. 3.2 LP) ;
- Participer, avec le CAIPRP, aux évaluations des facteurs relatifs à la vie privée requise par la Loi (art. 63.5 LAI et art. 3.3 et 3.4 LP) ;
- Répondre aux demandes de cessation de diffusion d'un renseignement personnel, de désindexation et de ré indexation d'hyperliens (art. 28.1 LP) ;
- Siéger sur le CAIPRP ;
- Être membre de l'équipe de gestion des incidents de confidentialité ;
- Recevoir l'avis sur une violation ou une tentative de violation par une personne de l'une ou l'autre des obligations relatives à la confidentialité d'un renseignement communiqué, et effectuer toute vérification relative à cette confidentialité dans le cadre de l'exécution d'un mandat ou contrat de services ou d'entreprise ;
- Tenir les registres de communications de renseignements personnels, incluant en cas d'incident de confidentialité **;**
- Mettre en place, avec le CAIPRP, des formations, des mécanismes de sensibilisation à la protection des renseignements personnels au sein de l'Ordre ;
- Répondre aux demandes de la Commission d'accès à l'information.

1.04 COMITÉ D'ACCÈS À L'INFORMATION ET DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le comité d'accès à l'information et de protection des renseignements personnels (CAIPRP) est mis sur pied par la présente politique et réuni :

- Le ou la directeur(trice) général(e) et secrétaire de l'Ordre, à titre de dirigeant(e) et responsable de la gouvernance ;
- Le ou la directeur(trice) des affaires juridiques et secrétaire adjoint(e) à titre de responsable de la gestion documentaire, de RPRP et de conseiller ou conseillère juridique ;
- Le ou la responsable des ressources matérielles et financières, à titre de responsable de la sécurité de l'information (RSI) ;
- Le ou la syndic(que) de l'Ordre, à titre de responsable à l'accès à l'information et à la protection des renseignements personnels pour le bureau du syndic.

Le CAIPRP peut s'adjoindre toutefois toute autre personne ayant une expertise ou des connaissances requises.

Le CAIPRP a pour mandat de soutenir l'Ordre dans l'exercice de ses responsabilités et dans l'exécution des obligations imposées par la LAI et la LP et est plus particulièrement responsable :

- D'approuver et mettre à jour périodiquement les règles encadrant la gouvernance que l'ordre doit adopter à l'égard des renseignements personnels ;
- D'élaborer un plan de révision des processus de collecte, d'utilisation, de transmission, de conservation et de destruction des renseignements personnels ;
- D'agir comme équipe de gestion des incidents de confidentialité en appliquant le plan prévu à cet effet ;
- D'être consulté dès le début de tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant le cycle de vie des renseignements personnels, aux fins de l'évaluation des facteurs relatifs à la vie privée et suggérer des mesures de protection des renseignements personnels applicables à ce projet.

1.05 ÉQUIPE DE GESTION D'UN INCIDENT DE CONFIDENTIALITÉ

Une équipe de gestion d'un incident de confidentialité est mise sur pied par la présente politique. Elle est composée des membres du CAIPRP et des personnes suivantes si l'incident de confidentialité implique la gestion d'une crise :

- ✓ La présidence ;
- ✓ La personne responsable des communications ;

L'équipe peut s'adjoindre de toute aide ou expertise requise (fournisseur informatique externe, spécialiste en cybersécurité, etc.).

L'équipe de gestion d'un incident de confidentialité a pour mandat d'adresser en priorité tout incident de confidentialité signalé et d'en assurer la prise en charge. Elle a notamment pour responsabilité de :

- Mettre en application le plan de gestion des incidents de confidentialité et la procédure afférente.
- Gérer tout incident de confidentialité.

1.06 AFFAIRES JURIDIQUES

Les affaires juridiques sont responsables de :

- Valider les politiques, les procédures ou les mesures appliquées du point de vue juridique ;
- S'assurer de la conformité des mesures mises en place par l'Ordre en matière de protection des renseignements personnels ;
- Informer ou conseiller les intervenants concernés dans le cas d'un incident de sécurité ou dans le cas d'une plainte ou d'un litige à l'endroit de l'Ordre.

1.07 RESPONSABLES DE SECTEURS ET LA SYNDIQUE

Les responsables de secteurs et le ou la syndic(que) sont responsables de :

- S'assurer que les requis en matière de gestion et protection de l'actif informationnel soient bien intégrés dans les processus d'affaires ;
- S'assurer que tout nouvel intervenant soit formé ;
- Veiller à la protection de l'actif informationnel sous sa responsabilité et de veiller au respect des règles en matière d'accès et de gestion des renseignements personnels ;
- Respecter et s'assurer du respect des directives et procédures en matière de gestion et de protection de l'actif informationnel.

1.08 TOUS LES INTERVENANTS

Tous les intervenants exercent aussi des responsabilités en matière de gestion et protection de l'actif informationnel. À cet effet, elles ou ils sont responsables de :

- Prendre connaissance et comprendre la Politique de gestion et protection de l'actif informationnel, ainsi que toute autre politique, procédure, guide d'application ;
- Participer activement aux séances d'information ou de formation ;
- Prendre connaissance et signer tout engagement de confidentialité ;
- Respecter les règles adoptées par l'Ordre en matière de protection des renseignements personnels, et ce, tout au long de leur cycle de vie ;
- Appliquer les règles et bonnes pratiques en matière de gestion ;
- Aviser sans délai le responsable de l'accès en cas d'incident de sécurité.

2.00 EXIGENCE DE LA POLITIQUE APPLICABLE À TOUT ACTIF INFORMATIONNEL

2.01 GESTION DES RISQUES

L'Ordre prend les moyens raisonnables afin de mettre en place des mesures de prévention, de détection et de protection visant à assurer la sécurité de son actif informationnel et le prémunir, autant que possible, de toute atteinte à sa confidentialité, à son intégrité, à sa disponibilité ou à sa traçabilité.

Les mesures prises à cet effet doivent permettre de mitiger la survenance d'un incident de sécurité ou les risques y étant associés et elles tiennent compte du degré de sensibilité de l'actif informationnel, et ce, à toute étape de son cycle de vie.

À cet effet, l'Ordre effectue, sur une base périodique et au besoin, un audit de ses systèmes informatiques, afin de veiller notamment à l'optimisation de la sécurité de son parc informatique.

2.02 GESTION DES ACCÈS À L'ACTIF INFORMATIONNEL

L'Ordre prend les mesures nécessaires pour assurer la protection de l'actif informationnel, dont les renseignements personnels, et ce, à toutes les étapes de leur cycle de vie. Les mesures visent notamment à assurer la confidentialité, leur intégralité, leur disponibilité et leur traçabilité.

L'accès de l'actif informationnel sur le plan numérique et physique est restreint aux personnes autorisées

et qui en ont besoin afin d'accomplir leur fonction. Les accès sont ainsi établis selon la nécessité et la sensibilité des renseignements contenus au dossier. Les accès octroyés aux divers employés de l'Ordre sont représentés à son plan de classification.

L'accès à l'actif informationnel informatisé de l'Ordre est contrôlé par l'authentification de l'utilisateur et un mot de passe unique associé à chaque intervenant. Chaque intervenant est responsable de ses codes d'authentification et ne doit en aucun temps les partager avec une personne non autorisée à les recevoir.

Chaque intervenant devrait également fermer sa session à la fin de chaque utilisation.

Les comptes informatiques des employés de l'Ordre sont également munis d'un système de double identification.

L'actif informationnel sur support papier qui revêt un certain niveau de confidentialité est conservé, sous clef, au siège de l'Ordre ou selon les dispositions prévues à la Politique sur le télétravail.

2.03 GESTION DES INCIDENTS DE SÉCURITÉ ET DE CONFIDENTIALITÉ

Tout intervenant a l'obligation de signaler immédiatement au RPRP et au RSI tout incident de sécurité avéré ou présumé. Il appartiendra au RPRP et l'équipe de gestion d'un incident de confidentialité de déterminer si l'incident de sécurité constitue un incident de confidentialité et si des mesures sont à prendre.

Un incident de sécurité signalé est traité selon la procédure établie à l'annexe 2.

Dans le cas où un incident de confidentialité doit être dénoncé, le RPRS en avise la Commission d'accès à l'information (CAI) et les personnes dont les renseignements personnels ont été compromis selon les modalités prévues au Règlement sur les incidents de confidentialité.

2.04 GESTION DES RENSEIGNEMENTS PERSONNELS

2.04.01 Collecte des renseignements personnels

L'Ordre recueille uniquement les renseignements personnels nécessaires aux finalités visées afin de réaliser sa mission de protection du public.

L'Ordre recueille les renseignements personnels principalement :

- Pour effectuer des paiements ;
- Pour répondre à certaines obligations à titre d'employeur ;
- Pour traiter une demande d'inscription, de réinscription ou de renouvellement au tableau de l'Ordre, d'inscription au registre des étudiants ;
- Pour traiter une demande d'équivalence de diplôme et de la formation, de reconnaissance de qualifications professionnelles en vertu d'un arrangement de reconnaissance mutuelle (ARM) ou encore dans le cadre d'une demande d'un permis spécial ;
- Pour traiter les dossiers de formation continue, l'inscription à des formations ou des activités de l'Ordre et pour accréditer des formations ;
- Pour effectuer les activités en lien avec l'inspection professionnelle ;

- Pour mener une enquête disciplinaire, une enquête en usurpation de titre ou en exercice illégal ;
- Pour transmettre des communications ;
- Pour effectuer les actions nécessaires dans le cadre des élections au Conseil d'administration de l'Ordre ;
- Pour traiter les candidatures pour les comités ou les groupes de travail de l'Ordre ou encore pour les postes au sein de l'Ordre ;
- Pour toute autre finalité.

Les renseignements personnels recueillis par l'Ordre concernent et proviennent principalement des membres, des étudiants et des candidats à la profession, mais peuvent également concerner et provenir des employés, des membres de comités, des administrateurs de l'Ordre ou encore des tiers (mandataires, fournisseurs, consultants, etc.). Les renseignements personnels peuvent inclure, mais sans limitation, le prénom, le nom, l'adresse, le numéro de téléphone, la date de naissance, le numéro d'assurance sociale, l'adresse courriel, l'adresse postale, le sexe, l'information relative à l'assurance responsabilité professionnelle, les informations bancaires, etc.

Lorsque la collecte de renseignements personnels est effectuée par un tiers (mandataires, fournisseurs, consultants, etc.) et pour le compte de l'Ordre, celui-ci s'assure contractuellement ou par d'autres moyens raisonnables que ces tiers respectent la Politique et mettent en place des mesures raisonnables pour assurer la protection des renseignements.

2.04.02 Utilisation

L'accès aux renseignements personnels est restreint aux personnes autorisées qui en ont besoin afin d'accomplir leurs obligations dans le cadre de leur fonction.

Un renseignement personnel est utilisé uniquement pour la ou les finalité(s) pour laquelle ou lesquelles il a été recueilli.

Un renseignement personnel peut également être utilisé lorsque cela est nécessaire à des fins d'étude, de recherche ou de production de statistiques. Le cas échéant, il est dépersonnalisé de manière à ne plus permettre d'identifier la personne concernée en supprimant notamment nom et prénom, adresse civique, courriel et numéros d'identification. L'Ordre prend alors les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de renseignements dépersonnalisés.

2.04.03 Communication

L'Ordre est responsable des renseignements personnels qu'il communique. Ainsi, il prend les mesures nécessaires pour en assurer la protection. Pour ce faire, lorsqu'il communique des renseignements personnels, il obtient les garanties suffisantes à cet effet. Ainsi, lorsque l'Ordre engage des tiers (mandataires, fournisseurs, consultants, etc.), lesquels peuvent avoir accès à des renseignements personnels dans le cadre de l'exécution de leurs services, l'Ordre s'assure contractuellement ou par d'autres moyens raisonnables que ces tiers respectent la politique et mettent en place des mesures raisonnables pour assurer la protection des renseignements.

Les renseignements personnels ne sont pas communiqués sauf lorsque les lois l'autorisent ou l'exigent. Uniquement les renseignements nécessaires aux finalités visées sont communiqués.

Une évaluation des facteurs relatifs à la vie privée est effectuée lorsque la loi le requiert. La communication, lorsqu'autorisée par la LAI ou la LP, est faite selon les conditions et modalités qu'elle prévoit le cas échéant.

2.04.04 Conservation et destruction des renseignements

Les renseignements personnels sont conservés selon un calendrier de conservation. Ainsi, un renseignement personnel est conservé pour la période nécessaire à la réalisation de la finalité pour laquelle il est recueilli.

Pour certains renseignements personnels, la loi prescrit la durée de conservation.

L'Ordre détruit les renseignements personnels lorsque la finalité pour laquelle il a été recueilli est réalisée. La destruction s'effectue selon une méthode adaptée selon le support et le niveau de confidentialité des documents.

Au lieu de les détruire, l'Ordre peut anonymiser les renseignements personnels pour les utiliser à des fins d'intérêt public. Le cas échéant, l'anonymisation est faite conformément au *Règlement sur l'anonymisation des renseignements personnels*.

L'Ordre prend les mesures raisonnables pour s'assurer de l'exactitude des renseignements personnels qu'il détient, c'est-à-dire qu'il s'assure qu'ils sont conformes et maintenus à jour selon les finalités pour lesquelles ils ont été recueillis.

2.04.05 Gestion des droits des personnes concernées et des plaintes relatives à la protection des renseignements personnels

Si une personne souhaite connaître les renseignements personnels que l'Ordre détient sur elle ou encore si elle veut procéder à une rectification de ceux-ci, elle doit s'adresser, par écrit, au responsable de la protection des renseignements personnels à l'adresse suivante : secretaire@ohdq.com.

L'Ordre reconnait que la personne concernée par des renseignements personnels peut se prévaloir de certains droits tels que :

- Droit d'être informée que ses renseignements sont recueillis ;
- Droit d'accès à ses renseignements personnels ;
- Droit de demander la rectification de tout renseignement personnel incomplet ou inexact ;
- Droit de demander la mise à jour des renseignements personnels ;
- Droit de demander l'effacement ou la limitation des renseignements personnels.

et veille à donner suite à toute demande à cet effet selon les modalités et conditions prévues par la LAI ou la LP.

Advenant le cas où une personne souhaite déposer une plainte quant à la protection que l'Ordre accorde aux renseignements personnels qu'il détient, celle-ci peut le faire en contactant le responsable de la protection des renseignements personnels par courriel à l'adresse suivante : secretaire@ohdq.com.

La plainte doit contenir les éléments suivants :

- Identification du plaignant : nom, coordonnées (courriel et adresse postale) ;
- Objet et motif de la plainte – la plainte doit suffisamment être précise ;

Le ou la RPRP doit, avec diligence et au plus tard dans les 30 jours qui suivent la réception de la plainte :

- Envoyer, par écrit, un accusé de réception au plaignant ;
- Analyser la recevabilité de la plainte ;
- Obtenir la collaboration des administrateurs, membres de la direction ou du personnel administratif de l'Ordre pour traiter la plainte et, le cas échéant, faire appel à des ressources externes ;
- Répondre, par écrit, au plaignant. La réponse doit :
    - Être motivée ;
    - Indiquer, le cas échéant, les mesures correctives prises pour modifier les pratiques et procédures visées par la plainte si celle-ci est jugée recevable ;
    - Indiquer le recours qui s'offre au plaignant si celui-ci entend contester la décision prise et les délais dans lesquels ils peuvent être exercés. Un recours en révision peut être exercé auprès du CAIPRP, à l'exclusion du RPRP ayant traité la plainte. Dans un tel, le CAIPRP peut s'adjoindre d'un conseiller ou d'une conseillère juridique externe.

Le ou la RPRP doit tenir un dossier pour chacune des plaintes reçues. Ce dossier doit contenir la plainte, l'analyse qui a été réalisée, la réponse transmise au plaignant et, le cas échéant, les mesures correctives qui ont été prises et les documents au soutien de la plainte.

2.04.06 Consentement

De manière générale, il est nécessaire d'obtenir le consentement de la personne concernée avant de recueillir ses renseignements personnels. Le consentement peut être donné de façon verbale ou écrite et varie selon les circonstances et le type de renseignements personnels. Le consentement écrit est à privilégier.

Le consentement peut être explicite ou implicite. Il est implicite lorsqu'il s'infère du contexte, par exemple lorsqu'une personne transmet à l'Ordre un formulaire dans lequel il inscrit des renseignements personnels.

L'Ordre recueille des renseignements personnels concernant une personne auprès de tiers lorsqu'il obtient le consentement de cette personne ou lorsque la loi lui permet ou l'oblige.

Avant de communiquer des renseignements personnels auprès de tiers, l'Ordre s'assure d'obtenir le consentement de la personne concernée. Toutefois, lorsque la loi lui permet ou l'oblige, l'Ordre peut communiquer des renseignements personnels la concernant à des tiers sans son consentement et selon les conditions et modalités que la loi prévoit.

Dans certains cas, la loi permet à l'Ordre de recueillir, utiliser, communiquer et conserver des renseignements personnels même si une personne le refuse. Ainsi certains renseignements ne sont pas confidentiels, revêtent un caractère public et l'Ordre peut les communiquer sans son autorisation. À titre d'exemple :

- Nom d'un membre ;

- Adresse et numéro de téléphone du domicile professionnel d'un membre de l'Ordre ;
- La mention du fait qu'un membre a déjà été radié ou que son permis est limité ou suspendu.

2.04.07 Sondage

Lorsque l'Ordre réalise lui-même ou lorsqu'il confie un mandat à l'externe pour réaliser un sondage impliquant des renseignements personnels, il procède au préalable, avec le concours du CAIPRP et du RPRP, à une évaluation :

- de la nécessité de recourir à un sondage ;
- des mesures à prendre pour assurer la sécurité des renseignements personnels recueillis ou utilisés lors du sondage, incluant le fait :
    - de conclure une entente avec l'entité externe qui réalise le sondage pour le compte de l'Ordre, le cas échéant ;
    - de prévoir les informations à transmettre aux personnes sondées, par exemple, indiquer que le sondage est réalisé par ou pour le compte de l'Ordre, des objectifs du sondage, des fins pour lesquelles des renseignements personnels sont recueillis, des catégories de personnes qui y auront accès, du caractère facultatif de participer au sondage, des recours offerts aux répondants et de la personne auprès de qui ils peuvent être exercés ;
    - de mettre en place des mécanismes pour s'assurer que les renseignements personnels recueillis dans le cadre du sondage soient détruits ou anonymisés dès que les finalités du sondage sont réalisées ;
- de l'aspect éthique du sondage compte tenu, notamment, de la nature du sondage, des personnes visées, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

À cet effet, le CAIPRP évalue les outils technologiques et applications que les membres du personnel peuvent employer pour effectuer de tels sondages après qu'une évaluation de la sécurité est faite. Les sondages produits par l'Ordre ou pour le compte de l'Ordre doivent limiter au strict nécessaire la collecte de renseignements personnels. Tout intervenant désirant effectuer un sondage doit, à cet effet, suivre la procédure prévue à l'annexe 3.

3.00 ÉVALUATION ET SUIVI DE L'APPLICATION DE LA POLITIQUE

3.01 RESPONSABILITÉ DE L'ÉVALUATION ET LE SUIVI DE L'APPLICATION DE LA POLITIQUE

Le CAIPRP assure l'évaluation et le suivi de l'application de la politique.

Il en fait rapport au Conseil d'administration.

3.02 RÉVISION DE LA POLITIQUE

Le ou la RPRP assure une vigie continue de l'application de la politique.

Une révision complète de la politique est effectuée tous les 5 ans ou au besoin selon les changements législatifs et réglementaires.

Les versions révisées sont soumises au Conseil d'administration pour adoption.

ANNEXE 1

ENGAGEMENT DE CONFIDENTIALITÉ DU PERSONNEL, DES CADRES ET DES MEMBRES DU CONSEIL D'ADMINISTRATION ET DES MEMBRES DE COMITÉ

Je, soussigné(e), _____, déclare avoir lu la Politique de gestion et protection de l'actif informationnel et en avoir bien compris son contenu.

À cet effet et en plus de mon serment de discrétion, je m'engage à respecter la confidentialité des renseignements personnels et des informations auxquels j'aurai accès dans l'exercice de mes fonctions et plus particulièrement à :

1. N'accéder qu'aux seuls renseignements personnels et informations confidentielles nécessaires à l'exécution de mes tâches dans le cadre de mes fonctions au sein de l'Ordre ;
2. n'utiliser ces renseignements personnels et informations confidentielles que dans le cadre de mes fonctions au sein de l'Ordre ;
3. Ne révéler aucun renseignement personnel ou information confidentielle dont je pourrais avoir pris connaissance dans l'exercice de mes fonctions à moins d'y être dûment autorisé(e) ;
4. Prendre les mesures de sécurité nécessaires pour assurer la confidentialité des renseignements personnels et des informations confidentielles auxquels j'aurai accès dans le cadre de l'exercice de mes fonctions, notamment en contrôlant les accès et en m'assurant de ne pas révéler mes codes d'accès et mots de passe ;
5. Informer sans délai mes supérieurs, le responsable de la protection des renseignements personnels et de la sécurité informationnelle de toute situation ou irrégularité qui pourraient compromettre de quelque façon la sécurité, l'intégrité ou la confidentialité des renseignements personnels ou de l'information confidentielle détenus par mon employeur ;
6. Ne conserver, au terme de mes fonctions ou de mon emploi au sein de l'Ordre, aucun renseignement personnel ou information confidentielle auquel j'aurai accès dans le cadre de mes fonctions et à en disposer selon les directives ou procédures en place.

Signé à _____ le _____

_____
Prénom et nom en lettre moulées

_____
Signature

ANNEXE 2

PROCÉDURE À SUIVRE EN CAS DE SIGNALEMENT D'UN INCIDENT DE SÉCURITÉ ET DE CONFIDENTIALITÉ

PROCÉDURE DE GESTION D'UN INCIDENT DE SÉCURITÉ ET DE CONFIDENTIALITÉ

PRÉAMBULE

L'Ordre des hygiénistes dentaires du Québec (ci-après « Ordre », « Nous ») reconnaît l'importance d'assurer la protection des renseignements personnels qu'il recueille auprès des candidats à la profession, de ses membres, de ses employés et de toute autre personne avec qui il est appelé à interagir dans le cadre de ses activités. À ce titre, l'Ordre est responsable de la protection des renseignements personnels qu'il détient ou qu'il confie, le cas échéant, à un tiers, et ce, tout au long du cycle de vie de ces renseignements.
L'Ordre prend les moyens nécessaires pour assurer la protection des renseignements personnels. Néanmoins, des incidents de confidentialité impliquant des renseignements personnels peuvent survenir. L'Ordre s'est doté de la présente procédure pour être en mesure de diminuer et de répondre adéquatement en cas d'incident de confidentialité.

1. Objectif et cadre juridique

La présente procédure a pour objectif d'établir les démarches à suivre lorsque l'Ordre a des motifs de croire que s'est produit un incident de confidentialité impliquant des renseignements personnels qu'il détient ou qu'il a confié à un tiers.

2. Cadre juridique

La présente procédure tient compte du cadre juridique applicable à l'Ordre en matière de protection des renseignements personnels, notamment :

- *Code des professions* (RLRQ, c. C-26)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels lorsque les renseignements personnels* (RLRQ, c. A-2.1) sont détenus dans le cadre du contrôle de l'exercice de la profession
- *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1) lorsque les renseignements personnels sont détenus dans le cadre de ses autres fonctions et activités
- *Règlement sur les incidents de confidentialité* (RLRQ, c. A-2.1, r. 3.1)

3. Champ d'application

La présente procédure s'applique aux employés, membres d'un comité, administrateurs de l'Ordre, mais aussi aux tiers auxquels l'Ordre communique des renseignements personnels, aux fournisseurs ou partenaires de l'Ordre, incluant les sous-traitant.

4. Définition

Aux fins de la présente procédure, on entend par :

- **Incident de confidentialité** : tout accès, utilisation ou communication non autorisée par la loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce renseignement.
    - *Exemples d'accès non autorisé par la loi*
        - *Consultation non autorisée / non nécessaire à l'exercice des fonctions des renseignements personnels par un employé ou par un fournisseur de service*
        - *Intrusion d'un tiers dans le système informatique de l'entreprise : hameçonnage, rançongiciel, etc.*
        - *Etc.*

- *Exemples d'utilisation non autorisée par la loi*
  - *Membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne*
  - *Consultation / extraction non autorisée de renseignements personnels*
  - *Etc.*
- *Exemples de communication non autorisée par la loi*
  - *Communication de renseignements personnels à la mauvaise personne*
  - *Etc.*

- **Personne concernée** : toute personne dont les Renseignements personnels sont visés par un Incident de confidentialité.
- **Personne liée** : employés, membres d'un comité, administrateurs de l'Ordre, tiers auxquels l'Ordre communique des renseignements personnels, fournisseurs ou partenaires de l'Ordre, incluant les sous-traitants.
- **Préjudice sérieux** : Acte ou évènement susceptible de porter atteinte à la Personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.
- **Renseignement personnel** : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
- **Responsable de la protection des renseignements personnels (RPRP)**: personne veillant à assurer le respect et la mise en œuvre du cadre juridique applicable à la protection des renseignements personnels au sein de l'Ordre.

5. Procédure à suivre

5.1. Signalement

Si une personne liée à l'Ordre a des raisons de croire qu'un incident de confidentialité impliquant des renseignements personnels s'est produit, elle doit en aviser, sans délai, le Responsable de la protection des renseignements personnels de l'Ordre et lui fournir toute information pertinente.
Il n'appartient pas à la personne liée de déterminer s'il s'agit ou non d'incident de confidentialité. Dans le doute, il est préférable qu'elle en avise le Responsable sans délai.

5.2. Évaluer la situation

Le ou la RPRP, avec la collaboration l'équipe de gestion d'un incident de confidentialité tel que constitué en vertu de l'article 1.05 de la Politique de gestion et protection de l'actif informationnel, doit :

- **Examiner** le signalement afin de **déterminer** s'il s'agit d'un incident de confidentialité impliquant des renseignements personnels.
  - *Exemples de questions à se poser :*
    - *Les informations visées par l'incident sont-elles des Renseignements personnels ?*
    - *Les Renseignements personnels ont-ils fait l'objet d'un accès, d'une utilisation ou d'une communication non autorisée par la loi ? ont-ils fait l'objet d'une perte ou de toute autre atteinte à leur protection ?*
- **Aviser** les intervenants concernés à l'interne afin d'identifier, de circonscrire, d'enquêter et de corriger la situation liée à l'incident de confidentialité.
  - Intervenants concernés : à savoir l'équipe de gestion tel que constitué en vertu de l'article 1.05 de la Politique de gestion et protection de l'actif informationnel, ainsi que toute personne susceptible de contribuer à l'enquête de l'équipe de gestion d'un incident de confidentialité. L'équipe de gestion d'un incident peut s'adjoindre de toute aide ou expertise requise (fournisseur informatique externe, spécialiste en cybersécurité, etc.) ;
  - *Exemples de questions à se poser :*
    - *Quelle est la cause de l'incident ?*

        - *Quelles est la date ou la période visée par l'incident ?*
        - *Quelles sont les renseignements personnels visés ?*
        - *Étaient-ils chiffrés / protégés par un mot de passe ?*
        - *Ont-ils été récupérés ou détruits ?*
        - *Qui sont les personnes concernées par l'incident ? Quel est leur nombre ?*
        - *Quelles sont les mesures de sécurité en place au moment de l'incident ?*
- **Aviser** la haute direction et si l'incident de confidentialité implique une gestion de crise, inclure la présidence et la personne responsable des communications ;
- Selon le degré de gravité de l'incident, en **informer** également dans les meilleurs délais le comité d'audit et le Conseil d'administration ;
- À tout évènement, **rendre compte** des incidents gérés 2 fois par année au comité d'audit et au Conseil d'administration.

5.3. Diminuer les risques – Limiter les atteintes à la vie privée

Le ou la RPRP, en collaboration avec l'équipe de gestion d'un incident de confidentialité, doit prendre rapidement les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

- *Exemples de mesures à prendre :*
    - *Récupérer ou exiger la destruction des Renseignements personnels impliqués*
    - *Révoquer ou modifier les mots de passe*
    - *Cesser la pratique non autorisée*
    - *Corriger les lacunes des systèmes informatiques*
    - *Contacter les personnes ou organismes à l'externe susceptibles de diminuer le risque de préjudice*

5.4. Identifier le risque de préjudice

Afin de déterminer si le préjudice est sérieux, le RPRP, en collaboration avec l'équipe de gestion d'un incident de confidentialité, doit identifier le risque de préjudice en tenant compte :

- de la **sensibilité** des Renseignements personnels
    - Renseignement de nature financière (Numéro de carte de crédit, de compte, de transit, information sur le soutien financier fourni par un ordre ou sur l'accommodation financière accordée, salaire, conditions d'emploi)
    - Renseignement de nature médicale
    - Renseignement d'identification (Numéro d'assurance sociale / maladie, permis de conduire)
    - Renseignement sur les origines ethniques, l'orientation sexuelle, l'identité de genre
    - Renseignement génétique ou biométrique
    - Etc.
- des **conséquences appréhendées** de l'utilisation des Renseignements
    - Vol d'identité
    - Fraude financière / Impact sur le dossier de crédit
    - Diffusion des renseignements personnels, notamment sensibles
    - Permanence / Perpétuation de l'atteinte
    - Répercussion sur la santé physique ou psychologique
    - Perte d'emploi
    - Humiliation, atteinte à la réputation, à la vie privée
    - Impact sur les relations professionnelles ou d'affaires
    - Etc.
- de la **probabilité** que les Renseignements soient utilisés à des fins préjudiciables.

5.5. Aviser les autorités compétentes et les personnes concernées

Le ou la RPRP doit :

- **Aviser la CAI**, avec diligence, en cas de préjudice sérieux
  - L'avis à la CAI doit être fait par écrit et contenir les éléments suivants (possible de remplir le formulaire prévu à cet effet sur le site de la CAI) :
    - le nom de l'Ordre;
    - le nom et les coordonnées de la personne à contacter au sein de l'Ordre relativement à l'incident ;
    - une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description ;
    - une brève description des circonstances de l'incident et, si elle est connue, sa cause;
    - la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période ;
    - la date ou la période au cours de laquelle l'Ordre a pris connaissance de l'incident;
    - le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres ;
    - une description des éléments qui amènent l'Ordre à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, telle que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables ;
    - les mesures que l'Ordre a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé ;
    - les mesures que l'Ordre a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que la date ou la période où les mesures ont été prises ou le délai d'exécution envisagé ;
    - le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.
- En cas de risque de préjudice sérieux, **aviser les personnes** dont les Renseignements personnels sont visés par l'incident de confidentialité.
  - L'avis à doit contenir les éléments suivants :
    - Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description ;
    - Une brève description des circonstances de l'incident ;
    - La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue ;
    - Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident ;
    - Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci ;
    - Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

- Cet avis n'a pas à être transmis aux personnes concernées tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.
- Cet avis peut être fait au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes :
  - lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée ;
  - lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'Ordre ;
  - lorsque l'Ordre n'a pas les coordonnées de la personne concernée.

  Un tel avis public peut aussi être rendu afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou pour l'atténuer.

- **Aviser les services de police, si requis ;**
- **Aviser les assureurs de l'Ordre ;**
- **Aviser les conseillers juridiques** pour obtenir des conseils relativement à la préservation de la preuve et aux risques juridiques associés aux mesures déployées
- Contacter les **personnes ou organismes à l'externe** susceptibles de diminuer le risque de préjudice. Si tel est le cas :
  - Ne communiquer que les renseignements personnels à cette fin ;
  - Enregistrer la communication.

5.6. Tenir un registre des incidents de confidentialité

Le RPRP veille à la tenue du registre qui contient l'ensemble des incidents de confidentialité, et ce, peu importe que le risque ait été qualifié de sérieux ou non.

Le registre doit contenir les éléments suivants :

- Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'Ordre doit inscrire la raison justifiant l'impossibilité de fournir cette description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue ;
- La date ou la période au cours de laquelle l'Ordre a pris connaissance de l'incident ;
- Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre ;
- Une description des éléments qui amènent l'Ordre à conclure qu'il y a, ou non, risque qu'un préjudice sérieux soit causé aux personnes concernées, comme :
  - la sensibilité des renseignements personnels concernés ;
  - les utilisations malveillantes possibles des renseignements ;
- les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables ;
- Les dates de transmission des avis à la Commission et aux personnes concernées, quand l'incident présente le risque de préjudice sérieux. L'Ordre doit aussi préciser si elle a donné des avis publics et la raison de ceux-ci ;
- Une brève description des mesures prises par l'Ordre à la suite de l'incident, pour diminuer les risques qu'un préjudice soit causé.

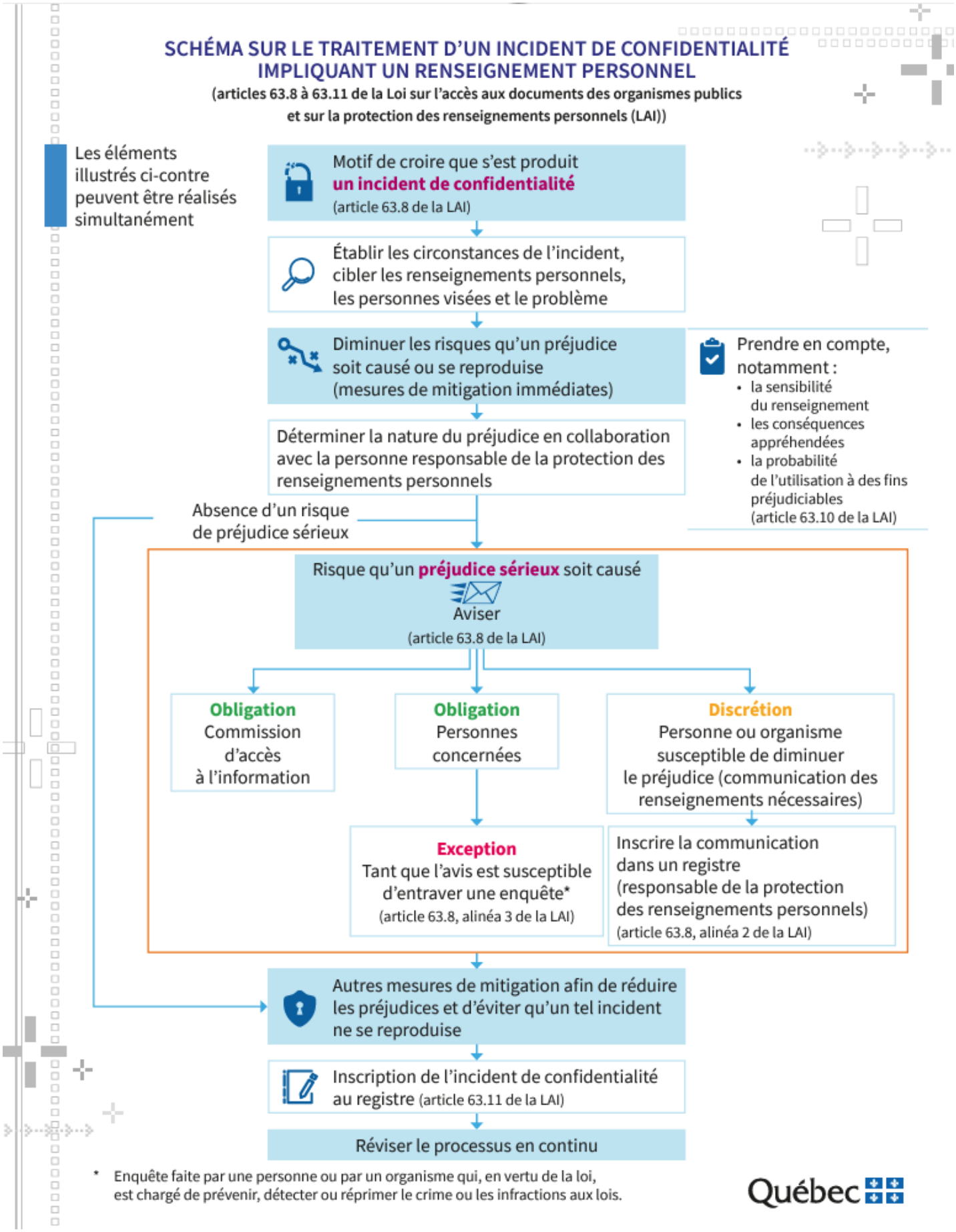
Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de 5 ans après la date ou la période au cours de laquelle l'Ordre a pris connaissance de l'incident.

5.7. Faire un suivi / un bilan de l'incident

Afin de tirer les leçons de l'incident de confidentialité, le ou la RPRP doit :

- Approfondir l'analyse des circonstances de l'incident ;
- Documenter – de manière chronologique – les actions prises en lien avec l'incident ;

- Réviser les procédures en place et, le cas échéant, en adopter de nouvelles ;



ANNEXE 3

PROCÉDURE À SUIVRE LORS DU RECOURS À UN SONDAGE

PROCÉDURE EN CAS DE RECOURS À UN SONDAGE

PRÉAMBULE

L'Ordre des hygiénistes dentaires du Québec (ci-après « Ordre », « Nous ») reconnaît l'importance d'assurer la protection des renseignements personnels qu'il recueille auprès des candidats à la profession, de ses membres, de ses employés et de toute autre personne avec qui il est appelé à interagir dans le cadre de ses activités. À ce titre, l'Ordre est responsable de la protection des renseignements personnels qu'il recueille, détient ou qu'il confie, le cas échéant, à un tiers, et ce, tout au long du cycle de vie de ces renseignements.
L'Ordre prend les moyens nécessaires pour assurer la protection des renseignements personnels, et ce, notamment dans le contexte de sondage que l'Ordre peut réaliser lui-même ou qu'il peut confier à des tiers. L'Ordre s'est doté de la présente procédure pour être en mesure de mener des sondages dans le respect de la législation et de la protection des renseignements personnels.

1. Objectif et cadre juridique

La présente procédure a pour objectif d'établir les démarches à suivre lorsque l'Ordre ou ses intervenants désirent recourir à un sondage pouvant comporter des renseignements personnels.

2. Cadre juridique

La présente procédure tient compte du cadre juridique applicable à l'Ordre en matière de protection des renseignements personnels, notamment :

- *Code des professions* (RLRQ, c. C-26)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels lorsque les renseignements personnels* (RLRQ, c. A-2.1) sont détenus dans le cadre du contrôle de l'exercice de la profession
- *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1) lorsque les renseignements personnels sont détenus dans le cadre de ses autres fonctions et activités;

3. Champ d'application

La présente procédure s'applique aux employés, membres d'un comité, administrateurs de l'Ordre, mais aussi aux tiers auxquels l'Ordre communique des renseignements personnels, aux fournisseurs ou partenaires de l'Ordre, incluant les sous-traitants. La présente procédure s'applique également dans le cas où un organisme ou une entreprise sollicite l'Ordre pour mener un sondage.

4. Définition

Aux fins de la présente procédure, on entend par :

- **Sondage** : enquête ou méthode statistique visant à donner une indication quantitative ou qualitative des opinions ou des comportements dans une population donnée.
- **Personne concernée** : toute personne qui souhaite réaliser un sondage pour le compte de l'Ordre, incluant ses employés, membres de comité et administrateurs.
- **Renseignement personnel** : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
- **Responsable de la protection des renseignements personnels (RPRP)**: personne veillant à assurer le respect et la mise en œuvre du cadre juridique applicable à la protection des renseignements personnels au sein de l'Ordre.

5. Procédure à suivre

5.1. Renseignements personnels et nécessité de recourir à un sondage

Une personne concernée qui souhaite recourir à un sondage dans le cadre de ses fonctions à l'Ordre et pour le compte de ce dernier doit déterminer :

- ✓ Si le recours à un sondage est nécessaire ou si l'information recherchée par le sondage peut être obtenue par un autre moyen (p. ex. : Extraction de données au Tableau de l'Ordre) ;
    - Pour évaluer la nécessité, il faut également déterminer si cela répond aux fins propres à la mission de l'Ordre p. ex. Cela contribue-t-il à assurer une meilleure protection du public, à assurer un meilleur encadrement de la profession, etc.
- ✓ Si des renseignements personnels seront communiqués ou collectés dans le cadre du sondage et s'il est nécessaire, dans un tel cas, de recueillir ces renseignements (p. ex. : Est-ce qu'un sondage anonymisé permettrait de répondre au besoin);

Si la réalisation du sondage projeté est nécessaire, mais n'implique aucunement la collecte ou le partage de renseignements personnels, il n'est pas requis de requérir l'évaluation du CAIPRP.
Si la réalisation du sondage est faite pour le compte d'un organisme ou une entreprise, la personne concernée doit soumettre cette demande au préalable auprès du CAIPRP qui devra procéder à une évaluation complète.

5.2. Évaluer la situation

Lorsqu'un sondage est requis et qu'il implique des renseignements personnels, la personne concernée doit en aviser le ou la RPRP avant d'entreprendre son sondage. Le ou la RPR, avec le concours du CAIPRP, procède alors à une évaluation :

- Obtenir les informations pertinentes de la personne ou du service concerné pour mener son évaluation, comme :
    - Les objectifs du sondage et la finalité recherchée ;
    - La nature des renseignements personnels qui seront communiqués ou recueillis dans le cadre du sondage projeté ;
    - La nature ou des exemples de questions qui seront posés dans le cadre du sondage;
    - Le moyen technologique (p. ex. : application Microsoft Forms) projeté pour mener le sondage ;
    - Le désir de recourir aux services d'un tiers pour mener le sondage.
- Réévaluer la nécessité ou non de procéder au sondage selon les critères suivants :
    - Les fins et l'objectif du sondage (sont-ils en cohésion avec les obligations de l'Ordre p. ex.?) ;
    - Les avantages de mener le sondage et les inconvénients s'il n'était pas mené ;
    - Les potentiels autres moyens d'obtenir les résultats ou l'information recherchée.
- Évaluer les mesures à prendre pour assurer la sécurité des renseignements personnels recueillis ou utilisés lors du sondage, incluant le fait :
    - de conclure une entente avec l'entité externe qui réalise le sondage pour le compte de l'Ordre, le cas échéant ;
    - de prévoir les informations à transmettre aux personnes sondées, par exemple, indiquer que le sondage est réalisé par ou pour le compte de l'Ordre, des objectifs du sondage, des fins pour lesquelles des renseignements personnels sont recueillis, des catégories de personnes qui y auront accès, du caractère facultatif

de participer au sondage, des recours offerts aux répondants et de la personne auprès de qui ils peuvent être exercés ;

Dans cette perspective, la personne concernée doit suivre les lignes directrices pour un consentement valide élaborées par la Commission d'accès à l'information.

- de mettre en place des mécanismes pour s'assurer que les renseignements personnels recueillis dans le cadre du sondage soient détruits ou anonymisés dès que les finalités du sondage sont réalisées ;
- De requérir un type de moyen technologique en particulier pour mener le sondage après une validation du CAIPRP concernant l'outil employé (p. ex. : applications comme Survey Monkey, Microsoft Forms, etc.) ;

- Évaluer l'aspect éthique du sondage compte tenu, notamment, de la nature du sondage, des personnes visées, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

5.3. Résultat de l'évaluation menée par le CAIPRP

Une fois son évaluation terminée, le CAIPRP, par l'entremise du RPRP, communique les résultats de cette évaluation à la personne concernée. Les résultats de cette évaluation peuvent mener le CAIPRP à :

- ✓ Autoriser le recours au sondage, mais en imposant certaines mesures ;
- ✓ Autoriser le recours au sondage, sans mesure particulière ;
- ✓ Refuser le recours au sondage.

ANNEXE 4

DÉCLARATION RELATIVE À L'ACTIF INFORMATIONNEL EN CAS DE FIN D'EMPLOI OU DE FIN DE FONCTIONS

Je, soussigné(e), _____, atteste que tout au cours de l'exercice de mon emploi ou de mes fonctions, j'ai respecté la Politique de gestion et protection de l'actif informationnel de l'Ordre, ainsi que toutes les procédures qui en découlent, et ce, au mieux de ma connaissance.

De plus, j'atteste qu'en date de la cessation de mon emploi ou de mes fonctions :

1. Ne plus avoir accès à l'actif informationnel de l'Ordre ;

2. Ne plus avoir en ma possession ou autrement conservé un quelconque actif informationnel de l'Ordre ;

3. Avoir détruit de façon irréversible tout actif informationnel de l'Ordre que j'aurais pu reproduire dans le cadre de mon emploi ou mes fonctions, et ce, autant ceux détenus sur support numérique que papier, après en avoir remis copie à l'Ordre, au besoin.

Signé à _____ le _____

_____
Prénom et nom en lettre moulées

_____
Signature