Ordre des dentistes du Québec

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

10 avril 2025

Table des matières

PRÉAMBULE

La mission de l'Ordre des dentistes du Québec (Ordre) est de protéger le public relativement à l'exercice de la profession de dentiste au Québec, conformément au Code des professions, RLRQ, c. C-26 (Code).

Afin de réaliser sa mission, l'Ordre recueille, crée, utilise et communique des informations sous plusieurs formes. L'Ordre reconnaît l'importance d'assurer la sécurité de ces informations qui ont une valeur légale, administrative ou économique, justifiant ainsi leur protection tout au cours de leur cycle de vie. L'Ordre s'engage donc à respecter les lois et règlements applicables à cet égard afin de maintenir un degré de sécurité approprié et ainsi de préserver la confidentialité et de garantir l'intégrité, la disponibilité et la traçabilité de ces informations.

Cette politique constitue le cadre de gouvernance de l'Ordre sur lequel il s'appuie pour réaliser ces objectifs. Elle décrit ses principes et pratiques en matière de sécurité de l'information.

LEXIQUE

Pour les fins de la politique, on entend par :

- **Actif informationnel** : une information, quel que soit son canal de communication (téléphonique, analogique, numérique, télégraphique, vocal ou autre), son support (papier, pellicule photographique, ruban magnétique, électronique ou autre), le système ou le support d'information, la technologie de l'information, l'installation ou un ensemble de ces éléments, acquis ou constitués par l'Ordre.
- **Disponibilité** : propriété d'une information d'être accessible en temps opportun, de la manière requise, par une personne ou une entité autorisée.
- **Équipe de la sécurité de l'information (ÉSI)** : collectif constitué de la direction générale adjointe et du secrétariat adjoint de l'Ordre, de la direction adjointe des technologies numériques, de la personne responsable de l'administration des systèmes et réseaux et d'une ou d'un technicien informatique.
- **Incident** : événement ne faisant pas partie du fonctionnement normal d'un service, quel que soit son mode de prestation, et qui entraîne ou peut entraîner une interruption ou une détérioration de la qualité de ce service.
- **Intégrité** : propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant la stabilité et la pérennité. L'intégrité fait référence à l'exactitude et à la complétude.
- **Intervenant** ou **utilisateur** : personne physique ou morale (p. ex. les membres du personnel, consultants, fournisseurs, clients, partenaires d'affaires et toute entité associée à l'Ordre ou qui en est mandataire) ayant accès, sur place ou à l'extérieur des locaux de l'Ordre, aux actifs informationnels, aux biens ou aux lieux pour lesquels l'Ordre a la responsabilité d'assurer la sécurité.
- **Membres du personnel** : employés de l'Ordre, contractuels, administrateurs, membres de comités ou de groupes de travail.
- **Renseignement confidentiel** : tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par une loi, dont les renseignements qui concernent une personne.
- **Responsable de la protection des renseignements personnels (RPRP)** : personne responsable de la gestion des incidents de confidentialité, de l'évaluation du préjudice sérieux et des avis obligatoires.
- **Traçabilité** : propriété associée à la conservation d'un document et de tout ce qui le compose, soit sa provenance, tout changement de support (informatique, papier, audio, visuel, numérique ou autre) et la piste des étapes du ou des processus ayant permis de créer ce document.

PORTÉE

La politique vise les actifs informationnels suivants, qu'ils soient situés dans les locaux de l'Ordre ou dans ceux d'un prestataire de services :

- l'information appartenant à l'Ordre ou détenue et exploitée par l'Ordre;
- l'information appartenant à l'Ordre et exploitée ou détenue par un tiers;
- l'information appartenant à un tiers et exploitée par lui au profit de l'Ordre.

Elle s'applique à tous les intervenants ou utilisateurs des actifs informationnels de l'Ordre.

La politique vise les activités impliquant la cueillette, la consultation, la production, la communication, la conservation et la destruction des actifs informationnels, peu importe leur emplacement ou le mode d'expression utilisé pour les rendre intelligibles, que ces activités soient conduites dans les locaux de l'Ordre ou dans un autre lieu.

CADRE JURIDIQUE

Cette politique est élaborée conformément aux lois et règlements qui encadrent la sécurité de l'information et s'appliquant aux ordres professionnels, tels que le Code civil du Québec, RLRQ, c. CCQ-1991, le Code des professions, RLRQ, c. C-26, la Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c. P.39-1, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1, et la Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1.

En cas d'incompatibilité entre les dispositions de la présente politique et celles des lois, ces dernières auront préséance.

CADRE ADMINISTRATIF

En complément à cette politique, l'Ordre a élaboré des politiques et directives encadrant sa gouvernance à l'égard de la sécurité de l'information, à savoir :

- Politique relative à la protection des renseignements personnels
- Directive sur la sécurité de l'information[1]
- Directive sur la sécurité TI[1]

[1] L'accès à ces documents est restreint puisqu'ils contiennent de l'information sensible, notamment en ce qui concerne les mesures déployées par l'Ordre pour assurer la sécurité.

RÔLES ET RESPONSABILITÉS

L'efficacité de la sécurité de l'information exige l'attribution claire de responsabilités à tous les niveaux de l'organisation. Elle nécessite en outre la mise en place d'un processus de gestion interne de la sécurité de l'information ainsi qu'une reddition de comptes adéquate.

Les responsabilités sont définies dans le tableau suivant :

Fonctions d'affaires	**Responsabilités**
Conseil d'administration	• Approuver la politique. • Assurer la protection et la confidentialité des actifs informationnels qu'il traite dans le cadre de ses fonctions, conformément aux principes énoncés dans cette politique. • Apporter les appuis financiers nécessaires pour la mise en œuvre et l'application de la présente politique et aligner les investissements et projets de sécurité de l'information avec les orientations stratégiques. • Participer aux activités de formation et de sensibilisation mises en place par l'Ordre.
Direction générale adjointe de l'Ordre	• S'assurer que les valeurs et les orientations en matière de sécurité de l'information sont partagées par l'ensemble des intervenants ou utilisateurs. • Élaborer et mettre à jour la présente politique et les directives, en collaboration avec la direction adjointe des technologies de l'information. • Assurer la définition, la mise en œuvre, l'organisation et l'évolution du cadre de gestion de la sécurité de l'information, en collaboration avec les différentes directions. • Définir les rôles et responsabilités des intervenants ou utilisateurs en regard de leur fonction relativement à la sécurité de l'information. • Assurer la réalisation et la mise en place des directives relativement au cadre de gestion de la sécurité de l'information. • S'assurer que chaque intervenant ou utilisateur reçoit une formation appropriée en matière de sécurité de l'information et adaptée à son usage des actifs informationnels. • Assurer le respect général de la politique et des directives de sécurité, tant d'un point de vue tactique qu'opérationnel, en vertu des orientations stratégiques. • Effectuer la reddition de comptes aux instances de l'Ordre.
Direction adjointe des technologies de l'information	• Élaborer et mettre à jour la présente politique et les directives, en collaboration avec la direction générale adjointe. • Assurer la sécurité des actifs informationnels en veillant à ce que les mesures de sécurité appropriées soient appliquées.

	• Proposer des plans d'atténuation des risques afin que les intervenants et utilisateurs puissent prendre les bonnes décisions et les protéger adéquatement. • Mesurer l'efficacité du système de gestion de la sécurité de l'information et proposer des pistes d'amélioration. • Développer et coordonner, avec la direction générale adjointe et la direction des ressources humaines et matérielles, les formations et campagnes de sensibilisation en matière de sécurité de l'information.
Ensemble des directions de l'Ordre	• Soutenir les déploiements et veiller au respect de la politique et des directives au sein de leur équipe. • S'assurer que leurs employés suivent les formations sur la sécurité de l'information mises en place par l'Ordre. • Signaler les incidents dont elles ont été informées au RPRP.
Intervenant ou utilisateur	• Utiliser les ressources informationnelles en se limitant aux fins pour lesquelles elles sont destinées et à l'intérieur des accès qui lui sont autorisés. • Respecter le caractère confidentiel des renseignements auxquels il a accès. • Assurer la sécurité des actifs informationnels de l'organisation au meilleur de ses connaissances et en fonction de ses rôles et responsabilités. • Aviser sans délai la RPRP de toute situation susceptible de compromettre la sécurité des actifs informationnels. • Consulter et respecter toutes les politiques et directives en lien avec la présente politique et édictées par l'Ordre. • Pour les membres du personnel seulement, participer aux activités de formation et de sensibilisation relatives à la protection des RP mises en place par l'Ordre.

PRINCIPES GÉNÉRAUX

L'Ordre assure la sécurité des informations conformément aux principes généraux suivants :

1. Norme ISO 27001 et PCI SSC 3.1

Les principes de base sur lesquels s'appuie la présente politique s'inspirent de la norme ISO 27001 et visent également à respecter les exigences relatives à la norme PCI Security Standards Council (SSC) 3.1.

2. Catégorisation des actifs informationnels

Les actifs informationnels sont catégorisés et inventoriés. Ils sont classifiés, protégés et détruits selon leur degré de sensibilité, le calendrier de conservation et les exigences qui y sont liées pour assurer leur sécurité.

3. Gestion du risque

Le choix des mesures de sécurité des actifs informationnels s'appuie sur l'identification et l'évaluation périodique des risques qui menacent la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information. Ainsi, les mesures de protection sont déployées en fonction de l'évaluation des impacts et de la probabilité d'occurrence d'une menace, et ce, de façon à atténuer les risques ou à les maintenir à un niveau acceptable.

4. Contrôle des accès

De manière à assurer la protection des informations, l'accès aux actifs informationnels est contrôlé pour empêcher tout accès non autorisé, tout dommage ou toute intrusion.

Les accès aux actifs informationnels sont attribués aux intervenants ou utilisateurs autorisés en fonction de ce qui leur est nécessaire pour accomplir leurs tâches, en tenant compte de leurs rôles et responsabilités. Une révision périodique des accès est prévue et effectuée par les gestionnaires des différentes directions, en collaboration avec l'ÉSI. Des règles d'utilisation des actifs informationnels sont édictées et des mécanismes de détection d'usages paraissant inappropriés sont mis en place aux termes de la Directive sur la sécurité de l'information.

5. Sécurité physique

Des mesures visant la sécurité des lieux physiques de l'Ordre sont également déployées afin de restreindre l'accès à des zones de l'organisation selon le degré de sensibilité des actifs qu'elles contiennent. Ces mesures protègent physiquement les actifs informationnels contre les menaces à la sécurité.

Ces mesures ont notamment pour objectif d'empêcher tout accès non autorisé aux équipements, installations et documents de l'Ordre. La sécurité physique porte autant sur le bâtiment et les locaux de l'Ordre, tels que les bureaux, la salle des serveurs et des équipements informatiques, le matériel de servitude, les équipements et

les supports informatiques, tels que les disques, disquettes et bandes magnétiques, les journaux et la documentation.

6. Formation et sensibilisation

L'aspect humain est un des éléments fondamentaux de la protection de l'information. La formation et la sensibilisation à la sécurité informationnelle de manière continue sont essentielles pour assurer la protection des informations.

Des activités de formation et de sensibilisation sont développées à cette fin, dont la Directive sur la sécurité de l'information, qui prévoit le rôle et les responsabilités des membres du personnel ainsi que les directives de sécurité existantes afin que chacun puisse développer ses réflexes et reconnaître les risques, les incidents et les possibles conséquences d'une atteinte à la sécurité.

Les membres du personnel peuvent également se référer à l'ÉSI pour obtenir des explications ou des renseignements supplémentaires quant aux modalités d'utilisation, de gestion et de protection des actifs informationnels.

7. Gestion de l'exploitation et des télécommunications

L'Ordre s'assure du maintien des infrastructures technologiques et prend les mesures de sécurité adéquates pour protéger les actifs informationnels afin de réduire au maximum les risques et d'offrir un environnement stable aux intervenants ou utilisateurs.

8. Acquisition, développement et entretien des systèmes d'information

Des mesures de sécurité sont établies et suivies tout au long du processus menant à l'acquisition, au développement, à l'implantation et à l'entretien des systèmes d'information. En outre, une évaluation des risques doit être effectuée avant de procéder à une acquisition liée aux systèmes d'information ou aux infrastructures informationnelles ou d'apporter des changements importants à ces derniers, comme le prévoit la Politique relative à la protection des renseignements personnels.

9. Continuité des activités

Dans l'éventualité d'un incident affectant les actifs informationnels jugés essentiels, l'Ordre doit s'assurer de la continuité des activités nécessaires à la réalisation de sa mission. Un plan de relève des services TI a été élaboré, lequel est validé et mis à jour annuellement afin de limiter les impacts advenant un incident majeur. L'application de ce plan de relève faciliterait la continuité et la reprise des activités essentielles dans les délais qui y sont prévus.

10. Signalement et gestion des incidents liés à la sécurité de l'information

Un processus complet de signalement et de gestion des incidents est documenté dans la Directive relative à la gestion des incidents de confidentialité. Conformément à celle-ci, tout intervenant ou utilisateur a l'obligation

de signaler, sans tarder, au RPRP tout acte susceptible de représenter une atteinte réelle ou présumée à la sécurité de l'information.

La mise en œuvre de ce processus de signalement et de gestion des incidents vise à traiter rapidement et efficacement tout événement qui cause ou pourrait causer un dommage ou entraîner la matérialisation d'un risque.

SANCTION

Lorsqu'un intervenant ou un utilisateur contrevient à cette politique, à ses directives ou à tout autre élément découlant de cette politique qui lui est applicable, il s'expose à des mesures administratives, disciplinaires ou légales en fonction de la gravité, du contexte et des conséquences de son geste. Ces mesures peuvent inclure la suspension des droits d'accès, la réprimande, la suspension, le congédiement ou autres.

REDDITION DE COMPTES

Tout document en lien avec cette politique doit être conservé avec soin, idéalement centralisé à un seul endroit, en format « natif » et dont l'intégrité a été préservée.

APPROBATION ET MODIFICATION

Cette politique a été adoptée par le conseil d'administration de l'Ordre et est entrée en vigueur dès son adoption.

L'Ordre se réserve le droit de modifier cette politique en tout temps.

Les dates d'adoption et de mise à jour sont indiquées ci-dessous.

Version	Date	Nature	Instance	Référence
1.0	2025-03-21	Adoption	CA	CA-21-03-25

800, boul. René-Lévesque Ouest, bureau 1640
Montréal (Québec) H3B 1X9

514 875-8511 | 1 800 361-4887

ODQ.QC.CA