POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Adoptée par le Conseil d'administration le 22 juin 2023

Ordre des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec

L'Humain avant tout

Ordre des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec
L'Humain avant tout

Classification	Politique de sécurité de l'information de l'OTSTCFQ
Adoption	Conseil d'administration Le 22 juin 2023 (résolution 2324-CA-036)
Mise à jour	
Responsable de l'élaboration et de la révision de la politique	Direction des finances, ressources humaines, technologie de l'information et services administratifs
Responsable de l'application de la politique	
Révision	Aux trois ans

Ordre des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec, 2023
255 boul. Crémazie Est, bureau 800,
Montréal (Québec) H2M 1L5
Tél. : 514-731-3925 / 1-888-731-9420

Table des matières

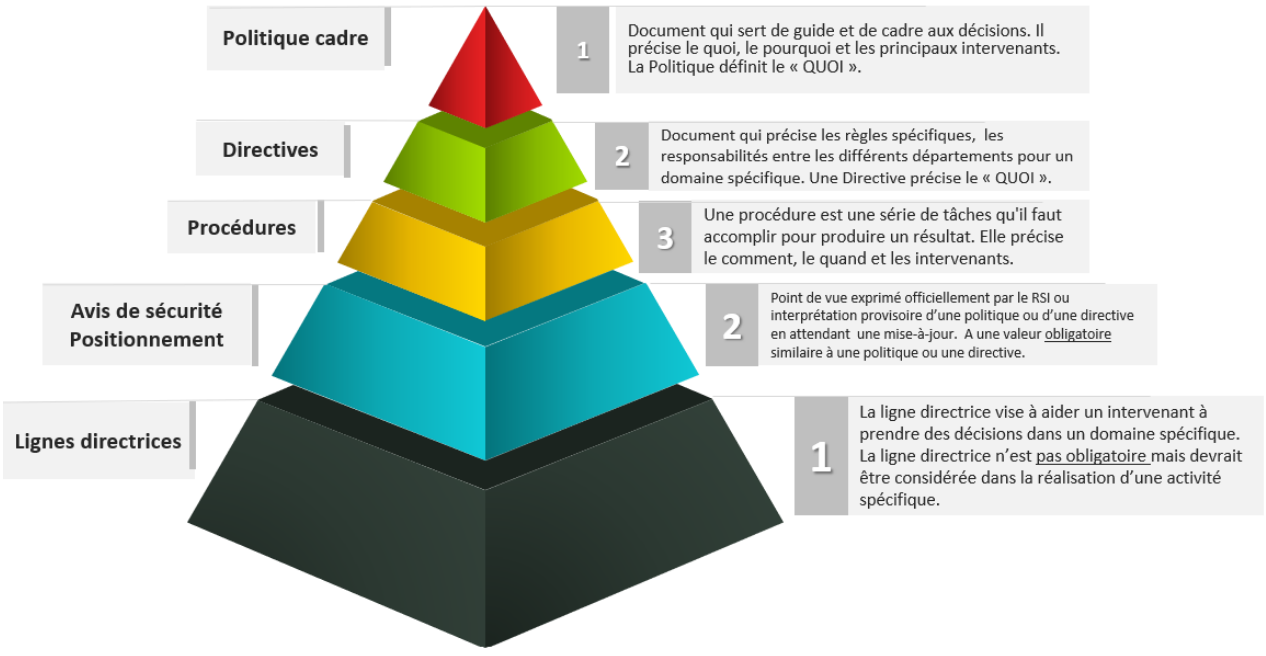
Préambule

Afin de mener à bien ses activités, l'Ordre des travailleurs sociaux et des thérapeutes conjugaux et familiaux du Québec (ci-après « l'Ordre ») génère, stocke, traite et communique des informations sous de nombreuses formes.

Il reconnaît que ces actifs informationnels, essentiels à son activité, doivent être évalués, utilisés de manière appropriée et protégés adéquatement tout au long de leur cycle de vie. L'Ordre adhère à la nécessité de protéger la confidentialité des renseignements personnels qu'il détient et au droit à la vie privée de son personnel et de ses membres. À cette fin, il est nécessaire de mettre en œuvre un ensemble cohérent de mesures de sécurité déterminées par une approche de gestion des risques de sécurité basée sur les meilleures pratiques, dans le respect des exigences législatives et réglementaires.

Les actifs informationnels couverts par la présente politique de sécurité comprennent non seulement les informations, mais aussi les équipements et les supports (papier ou numériques). Ils comprennent les données, les documents, les liens de communication interne, les sites d'hébergement, les technologies informatiques (TI), les appareils mobiles et autres équipements portables.

La politique représente un objectif à atteindre par l'Ordre dans les trois (3) ans suivant son adoption.



Introduction

Définitions

Les définitions des différents termes utilisés dans cette politique et dans d'autres documents associés sont disponibles dans le glossaire de la sécurité de l'information.

Objectifs

Le présent document constitue la politique de sécurité des actifs informationnels de l'Ordre (ci-après la « politique ») qui établit les pratiques à adopter pour se conformer à diverses obligations légales et administratives et pour protéger tous les actifs informationnels et prévenir les incidents de sécurité potentiels, notamment la fraude, les fuites d'information, les attaques informatiques, les erreurs accidentelles, les actions délibérées et les atteintes à la vie privée. De cette manière, l'Ordre protège ses actifs et atténue les risques liés à la confidentialité, à l'intégrité et à la disponibilité des informations.

Portée

Cette politique s'applique à tout actif informationnel détenu par l'Ordre y compris les informations recueillies dans le cadre d'activités contractuelles, réglementaires et légales. Sans limiter ce qui précède, aux fins de la présente politique, seront considérés comme des parties prenantes de l'Ordre, son personnel, ses membres du Conseil d'administration et de comités, ses sous-traitants, ses fournisseurs et toutes autres personnes intervenant dans les activités de l'Ordre.

Engagement du Conseil d'administration

Cette politique s'inscrit dans une démarche globale de prévention et de sensibilisation à la sécurité de l'information. Pour ce faire, la collaboration de tous les intervenants et intervenantes est essentielle. Le Conseil d'administration s'engage à prendre tous les moyens nécessaires pour soutenir les actions qui doivent être prises dans la mise en œuvre de cette politique, ainsi que dans la mise en œuvre des encadrements associés.

Propriétaire de la politique et du cadre de sécurité de soutien

La présente politique et les différents encadrements de sécurité associés relèvent de la personne responsable de la sécurité de l'information. Celle-ci doit en assurer la maintenance, la révision et la communication.

Suivi et contrôle des activités de sécurité de l'information

Afin de surveiller son exposition aux risques, l'Ordre doit disposer d'une infrastructure et de processus de surveillance.

Elle doit permettre de contrôler en permanence l'efficacité de ses méthodes, processus et mécanismes de protection et de les améliorer en fonction de l'évolution des risques auxquels l'Ordre est confronté.

L'Ordre se réserve le droit, sans préavis, de surveiller tout actif informationnel et toute information détenue, traitée et exécutée sur ses systèmes et appareils mobiles. Ce privilège doit toujours être exercé dans le respect des lois et lorsque des motifs raisonnables le recommandent.

Conséquences

Le non-respect de la présente politique ou des encadrements de sécurité associés peut amener l'Ordre à retirer les droits d'accès à son personnel, ses membres du Conseil d'administration et de comités, ses sous-traitants, ses fournisseurs et toutes autres personnes intervenant ainsi qu'à appliquer des mesures disciplinaires ou juridiques, selon le cas. Toute partie prenante qui a connaissance de la non-conformité ou de l'omission de cette politique doit en informer son ou sa responsable ou la personne responsable de la sécurité de l'information.

Respect de la politique

Les encadrements doivent être appliqués à l'appui des besoins d'affaires de l'Ordre et ne doivent en aucun cas devenir une contrainte sans valeur ajoutée ou empêchant l'Ordre d'offrir ses services à ses clients.

Compte tenu de ce qui précède, il est possible que, dans le cours normal des opérations, des situations spécifiques rendent impossible le respect de certaines exigences en matière de sécurité de l'information. Dans un tel contexte, une procédure claire de gestion des non-conformités aux exigences de sécurité est nécessaire pour s'assurer qu'elles sont correctement analysées, approuvées et suivies.

Principes généraux

Organisation interne

Afin d'assurer une gestion efficace de la sécurité de l'information au sein de l'Ordre, il est important de définir la structure organisationnelle soutenant la planification, le développement, la mise en œuvre et le contrôle des mesures de sécurité. La direction générale est chargée de veiller à ce que cette structure organisationnelle soit définie et mise en œuvre.

Évaluation et gestion des risques liés aux actifs informationnels

Outre la gestion des risques de l'organisation, les mesures de sécurité mises en place sont fondées sur l'évaluation, l'analyse périodique et le traitement par l'Ordre des risques liés à la confidentialité, à l'intégrité et à la disponibilité des informations.

Une évaluation des risques doit être réalisée avant de procéder à l'acquisition de nouveaux systèmes ou d'effectuer un changement susceptible d'avoir un impact sur la sécurité des actifs informationnels de l'Ordre. Dans tous les cas, cette évaluation doit être documentée en suivant un processus défini.

Sécurité des ressources humaines

L'Ordre doit établir des processus de sécurité des ressources humaines dans le but de réduire le risque d'erreur humaine, de vol, de fraude ou d'utilisation abusive des actifs informationnels de l'Ordre avant l'embauche, pendant la période d'emploi et après le départ d'un membre du personnel, de ses membres du Conseil d'administration et de comités et toutes autres personnes agissant à titre d'intervenant.

Gestion des actifs informationnels

Afin de mettre en place et de maintenir une protection appropriée, chaque actif informationnel doit être inventorié et attribué à un propriétaire qui connaît sa valeur et son importance pour l'Ordre. Le propriétaire établira sa classification en fonction de sa valeur et de son importance pour l'Ordre afin d'établir un niveau de protection approprié.

Contrôle d'accès aux actifs informationnels

Principe du « besoin de savoir »

Les informations ne doivent être divulguées qu'aux personnes qui ont besoin de ces informations dans le cadre de leurs fonctions et conformément aux obligations législatives et réglementaires.

Gestion de l'accès

La gestion des accès doit être effectuée selon des procédures et des processus formels, convenus et communiqués aux personnes concernées.

Lors d'un changement de poste (notamment en cas de mutation ou de promotion) ou lors d'un arrêt de travail, de cessation d'emploi, de contrat ou de mandat (licenciement, congé de longue durée, etc.) les accès seront revus.

Les propriétaires, en collaboration avec la personne responsable de la sécurité de l'information, doivent veiller à ce qu'un examen périodique des comptes d'utilisateurs et d'utilisatrices soit effectué.

Contrôles d'accès

Tout actif informationnel qui conserve des informations non classées comme publiques doit disposer d'un mécanisme d'authentification actif pour garantir que ces informations ne sont pas indûment divulguées, modifiées, supprimées ou rendues indisponibles.

Les utilisateurs et utilisatrices doivent disposer d'un identifiant unique et ne doivent en aucun cas le partager.

Sécurité physique et environnementale

Tous les actifs informationnels doivent être protégés par des mesures de sécurité physique en fonction de leur niveau de sécurité, des risques associés ainsi que de leur valeur pour l'Ordre.

L'accès aux bureaux et aux salles informatiques contenant des informations non classées comme publiques doit être physiquement limité par un mécanisme de sécurité approprié.

Gestion des opérations informatiques et télécommunications

À moins qu'elles n'aient été désignées comme « publiques », toutes les informations doivent être protégées contre toute divulgation non autorisée à des tiers. Les tiers peuvent avoir accès aux informations non classées comme publiques uniquement si un besoin a été démontré et si cette divulgation a été autorisée par le propriétaire ou par la loi.

Acquisition, développement et mise à jour des systèmes

Les exigences de sécurité à respecter lors de l'acquisition, du développement, de la mise en œuvre et de la maintenance d'un actif informationnel doivent être déterminées.

Les exigences de sécurité doivent tenir compte des évolutions technologiques et des nouveaux défis en matière de sécurité.

Gestion des incidents

L’Ordre doit établir et définir les responsabilités et les procédures à mettre en œuvre en cas d'incident de sécurité afin de garantir une réponse efficace et pertinente tout en assurant la mise en place d'une équipe capable de traiter les incidents.

Reprise après sinistre

L’Ordre doit mettre en œuvre un plan de reprise des technologies de l'information (ci-après, « plan de reprise après sinistre »") visant à réduire l'impact de l'indisponibilité d'un actif informationnel et à assurer ainsi une reprise des opérations dans les meilleurs délais. Les mesures de récupération doivent être vérifiées périodiquement afin de s'assurer de leur efficacité et de leur pertinence.

Formation et sensibilisation

L'Ordre doit informer le personnel, ses membres du Conseil d'administration et de comités des menaces et des conséquences d'une violation de la sécurité afin que chacun puisse reconnaître les situations à risque et agir en conséquence.

L'Ordre doit également fournir une formation spécialisée dans les domaines liés à la sécurité de l'information afin de maintenir un niveau de risque acceptable au sein de l'Ordre.

Un programme de formation et de sensibilisation à la sécurité de l'information adapté aux différents rôles du personnel, des membres du Conseil d'administration et de comités doit être défini.

Il incombe à l'Ordre de fournir à toute personne devant accéder aux actifs informationnels les directives nécessaires pour comprendre ses responsabilités en matière de sécurité de l'information.

Tous les documents pertinents doivent être communiqués incluant la présente politique et les encadrements associés.

Rôles et responsabilités

Conseil d'administration

Le Conseil d'administration de l'Ordre est chargé de veiller à ce que des encadrements de sécurité adéquats soient élaborés et maintenus au sein de l'Ordre. Le Conseil d'administration est chargé d'approuver cette politique et de prendre tous les moyens nécessaires pour la mettre en œuvre ainsi que les autres documents associés.

Responsable de la sécurité de l'information

La personne responsable de la sécurité de l'information est la principale représentante de l'Ordre pour toutes les questions relatives à la sécurité des actifs informationnels.

Sans limiter la généralité de ce qui précède, la personne responsable de la sécurité de l'information doit, entre autres choses :

- Rendre compte chaque année au comité d'audit, des finances, des technologies de l'information et de la gestion des risques (CAFTIGR) de la conformité à la politique et soumettre un rapport de conformité.
- Tenir la politique à jour en fonction des besoins, des obligations et des préoccupations de l'Ordre.
- Veiller à l'implication des différentes parties prenantes dans l'élaboration de cette politique et des autres encadrements associés.

- Définir les critères de sécurité pour les technologies utilisées au sein de l'Ordre.
- Fournir des conseils en matière de sécurité informatique.
- Réaliser des évaluations des risques et des vulnérabilités dans tous les projets impliquant un actif informationnel permettant de définir les besoins de sécurité pour assurer la protection des actifs informationnels.
- Sensibiliser tous les utilisateurs et utilisatrices à la sécurité des informations.
- Assurer une gestion efficace des incidents de sécurité et la maintenance du plan de reprise après sinistre basé sur le plan de continuité des activités.

Propriétaire de l'actif informationnel

Le propriétaire des actifs informationnels est la personne responsable d'un secteur d'activité de l'Ordre. Elle est responsable, d'un point de vue affaires des actifs informationnels qui sont nécessaires à la conduite des activités de sa direction, à savoir :

- Déterminer la valeur de ses actifs informationnels pour sa gestion et assurer leur classification conformément à celle-ci.
- Identifier et assurer la mise en œuvre de mesures et de contrôles de sécurité pour garantir la protection des actifs informationnels en fonction du niveau de sécurité attribué et des évaluations des risques.
- Assurer le maintien des mesures de sécurité pour tous ses actifs tout au long de leur cycle de vie (création, entretien, conservation, destruction, etc.).
- Approuver l'attribution des droits d'accès aux actifs informationnels sous sa responsabilité en fonction des besoins requis.
- S'assurer qu'un plan de reprise après sinistre, spécifique à ses actifs informationnels, est en place et est testé régulièrement.

Utilisateur ou utilisatrice d'un actif informationnel

L'utilisateur ou l'utilisatrice d'un actif informationnel est une personne à qui un propriétaire a accordé l'accès à un ou plusieurs actifs informationnels de l'Ordre. Celle-ci peut être un membre du personnel permanent, temporaire ou occasionnel, un membre du Conseil d'administration ou d'un comité, un·e contractuel·le, un·e consultant·e ou un tiers.

Lorsque la valeur de l'actif informationnel le justifie, des arrangements spéciaux avec un tiers (tels que des accords de confidentialité) doivent avoir été conclus avant l'attribution ou la cession du contrat.

Son rôle consiste, entre autres, à effectuer les tâches suivantes :

- N'utiliser les actifs informationnels qu'à des fins expressément définies par le propriétaire.
- Respecter toutes les mesures de sécurité en place.

- S'abstenir de divulguer les informations en leur possession (sauf si elles ont été désignées comme publiques) sans l'autorisation du propriétaire.
- Informer la personne responsable de la sécurité de l'information de toutes les situations où il ou elle pense que la sécurité d'un actif informationnel est vulnérable ou a été compromise.
- Se conformer à la présente politique et à tout autre document qui s'y réfère ou la soutient.

Entrée en vigueur et révision

La présente politique entre en vigueur le 22 juin 2023. Elle annule et remplace tous les encadrements à ce sujet précédemment en vigueur. Elle peut être révisée à tout moment par la personne responsable de la sécurité de l'information de l'Ordre. Toute révision de la politique doit être approuvée par le Conseil d'administration.

Des modifications de la politique ou de ses encadrements associés peuvent être proposées par les différentes parties prenantes de l'Ordre, qui doivent les soumettre par écrit à la personne responsable de la sécurité de l'information.

La présente politique et tous autres encadrements de sécurité associés doivent être revus au moins tous les trois (3) ans afin de garantir leur pertinence.

***