ARSF
Autorité ontarienne de réglementation des services financiers

# Information

**Date d'entrée en vigueur :** 18 août 2022
**Identifiant :** Nº MB0048INF

# Principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires pour le secteur du courtage d'hypothèques

## Objectif

La présente ligne directrice fournit des renseignements sur l'Autorité ontarienne de réglementation des services financiers (ARSF) concernant :

- l'adoption par l'ARSF des principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires (« directive de cybersécurité du CCARCH ») dans son cadre réglementaire;
- le « protocole de surveillance des pratiques de l'industrie en matière de cybersécurité », qui est activé afin d'établir un dialogue avec les titulaires de permis qui font face à un incident lié à la cybersécurité qui pourrait avoir un effet important sur les renseignements des clients.

La directive de cybersécurité du CCARCH a été élaborée en vue d'améliorer la préparation à la cybersécurité dans le secteur du courtage d'hypothèques en proposant des pratiques de pointe de prévention des incidents de cybersécurité et de réponse appropriée lorsqu'ils se produisent.

# Portée

La présente ligne directrice concerne les personnes et les entités suivantes qui sont réglementées par l'ARSF :

- les agents en hypothèques;
- les courtiers en hypothèques;
- les maisons de courtage d'hypothèques;
- les administrateurs d'hypothèques.

# Justification et contexte

Les cyberattaques représentent un risque important dans les secteurs réglementés par l'ARSF. Elles risquent de perturber ou de compromettre le flux d'informations entre les maisons de courtage d'hypothèques, les administrateurs d'hypothèques, les prêteurs/investisseurs, les emprunteurs et les fournisseurs de services tiers.

La cybersécurité est l'application de technologies, de processus et de contrôles pour protéger les infrastructures telles que les systèmes, les réseaux, les programmes, les appareils et les données. Elle vise à réduire la probabilité et les conséquences des cyberattaques qui pourraient mener à un accès non autorisé aux renseignements confidentiels des clients et à une perturbation des activités commerciales en raison de l'interférence avec les infrastructures critiques et les réseaux d'entreprise.

Pour certaines entités, la gestion des risques liés à la cybersécurité devrait faire partie des politiques et procédures de gestion des risques liés aux technologies de l'information (TI), visant à atténuer les menaces internes et externes pesant sur leurs systèmes informatiques, infrastructures et données.

La directive en matière de cybersécurité du CCARCH, et l'adoption de cette directive par l'ARSF, vise à soutenir la préparation à la cybersécurité dans le secteur du courtage d'hypothèques en proposant des pratiques de pointe de prévention des cyberincidents et des réponses appropriées lorsqu'ils se produisent.

En tant qu'autorité de réglementation des pratiques de l'industrie, l'ARSF a pour objectif de protéger l'accès non autorisé aux renseignements confidentiels des clients. Aux fins de la présente ligne directrice, s'entend par renseignements des clients tous les renseignements

relatifs aux consommateurs, y compris les emprunteurs, les prêteurs/investisseurs et les clients potentiels.

## Mandat de l'ARSF

En supervisant et en réglementant le secteur du courtage d'hypothèques, l'ARSF vise à atteindre ses objectifs statutaires qui, aux fins de la présente ligne directrice, sont les suivants :

- Renforcer la confiance du public envers le secteur du courtage d'hypothèques
- Surveiller et évaluer les tendances dans le secteur du courtage d'hypothèques
- Coopérer et collaborer avec les autres organismes de réglementation, le cas échéant
- Protéger les droits et les intérêts des consommateurs

# Information

## Cadre juridique pour les renseignements personnels

Le cadre juridique canadien exige que les renseignements personnels soient protégés. En vertu de la *Loi fédérale sur la protection des renseignements personnels et les documents électroniques* et du projet de *Loi fédérale sur la protection de la vie privée des consommateurs*, toutes les entreprises, y compris les maisons de courtage et les administrateurs d'hypothèques, ont l'obligation de protéger certains des renseignements personnels des clients. Par exemple, les données personnelles recueillies doivent être conservées en toute sécurité et protégées contre la perte, l'accès non autorisé et le vol de données.

## Code de conduite du CCARCH pour le secteur du courtage d'hypothèques

En vertu du principe 8 du Code de conduite du CCARCH pour le secteur du courtage d'hypothèques, « Les personnes et les entités réglementées doivent protéger les renseignements relatifs à leurs clients et doivent utiliser et divulguer ces renseignements uniquement aux fins pour lesquelles les clients ont donné leur consentement ou si la loi l'exige. »

## Directive de cybersécurité du CCARCH

Pour aider les entités titulaires d'un permis de l'ARSF à s'acquitter de leurs obligations et à gérer efficacement les risques liés à la cybersécurité, l'ARSF s'attend à ce qu'elles mettent en œuvre les « principes » indiqués dans la directive de cybersécurité du CCARCH. Ceux-ci décrivent les objectifs à atteindre pour être prêt en ce qui concerne la cybersécurité, sans toutefois en prescrire la manière de les atteindre. Cette approche permet aux entités réglementées de suivre une trajectoire de préparation adaptée à la taille et à la structure de leurs activités.

La directive de cybersécurité du CCARCH comprend une liste de contrôle pour aider les entités à évaluer leur état de préparation à la cybersécurité.

## Exigence en matière de formation continue

En vertu de l'article 9 du Règlement de l'Ontario 409/07 (Règl. de l'Ont. 409/07) pris en application de la *Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs hypothécaires et les administrateurs d'hypothèques*, l'ARSF a le pouvoir d'établir des exigences en matière de formation continue pour les agents et les courtiers en hypothèques. Les agents et les courtiers qui souhaitent renouveler leur permis doivent satisfaire à l'exigence de formation continue approuvée par le directeur général de l'ARSF.

Les exigences de formation continue de l'ARSF prévoient une formation et des sujets relatifs à la cybersécurité, au besoin. L'objectif de cette formation continue est que chaque titulaire de permis sache reconnaître les menaces en matière de cybersécurité et puisse prendre des mesures pour s'en protéger. Pour les maisons de courtage d'hypothèques et les administrateurs, l'ARSF souhaite soutenir l'industrie en veillant à ce que des processus soient en place pour reconnaître les risques liés à la cybersécurité, les surveiller et y répondre afin de protéger les renseignements des clients.

# Protocole de surveillance des pratiques de l'industrie de l'ARSF en matière de cybersécurité

## Notification des incidents liés à la cybersécurité

Les maisons de courtage d'hypothèques et les administrateurs d'hypothèques doivent informer[1] l'ARSF en envoyant par courriel le Formulaire d'avis d'incident découlant de risques liés aux TI à ITriskinbox@fsrao.ca ou en le téléchargeant, ainsi que tout autre document à l'appui, sur le Portail d'avis d'incident, s'ils sont confrontés à un incident de cybersécurité susceptible d'avoir des répercussions importantes sur les renseignements des clients.

L'ARSF veut s'assurer de ce qui suit :

- Des mesures appropriées sont prises pour protéger les clients.
- L'organisme de réglementation possède des renseignements à jour pour répondre à toute question du public.
- Les messages de l'organisme de réglementation et du titulaire de permis sont cohérents, afin d'éviter toute alarme indue.

L'organisme de réglementation devrait être informé dès que le titulaire de permis détermine qu'un incident lié à la cybersécurité pourrait avoir des conséquences importantes pour les clients. Voici quelques indicateurs d'un tel incident :

- L'atteinte à la sécurité touche un système ou une base de données qui stocke une grande quantité ou une proportion importante de renseignements confidentiels sur les clients.
- Dans le cours normal de ses activités, la maison de courtage ou l'administrateur d'hypothèques transmettrait le problème à la haute direction responsable de la sécurité de l'information ou l'informerait.
- L'incident nécessite des mesures ou des ressources non habituelles de la part de la maison de courtage ou de l'administrateur d'hypothèques.
- L'incident a mené à une demande d'indemnisation d'assurance.
- L'atteinte est un incident répété et pourrait avoir des conséquences importantes en cumulé.

[1] Auparavant, l'avis d'incident découlant d'un problème de cybersécurité était communiqué à l'ARSF par courrier électronique à l'adresse suivante : MBconduct@fsrao.ca.

**Activation du protocole de surveillance des pratiques de l'industrie de l'ARSF en matière de cybersécurité**

Lorsque l'ARSF prend connaissance d'un incident lié à la cybersécurité, suite à une information d'un titulaire de permis, à la veille commerciale, à un tuyau ou à une plainte, elle active son *Protocole de surveillance des pratiques de l'industrie en matière de cybersécurité*.

Le protocole décrit les échanges attendus entre l'ARSF et le titulaire de permis[2] afin de surveiller les actions de l'entité lors de l'enquête et de la réponse à l'incident. Le dialogue doit se poursuivre jusqu'à que l'ARSF ait :

- une compréhension et une connaissance complètes de l'étendue de l'atteinte potentielle des données et des renseignements qui ont pu être consultés;
- la confirmation que tout renseignement corrompu a été restauré, que l'atteinte a été rectifiée ou contenue, ou les deux;
- la confirmation que tous les systèmes sont revenus en ligne et sont complètement fonctionnels;
- la confirmation que tous les intervenants concernés, y compris les clients et les autorités compétentes en matière de protection de la vie privée, ont été informés, et que des mesures raisonnables ont été prises par le titulaire de permis pour limiter le préjudice potentiel causé aux clients;
- une compréhension et une connaissance complètes des mesures de protection qui ont été mises en place pour s'assurer que le titulaire de permis est protégé contre des atteintes futures similaires.

L'ARSF maintiendra la confidentialité des incidents signalés dans la mesure permise par la loi.

La réponse aux incidents se déroule généralement par phases, de façon semblable à ce qui suit :

**Phase 1 :** Réception immédiate des renseignements du titulaire de permis sur ce qu'il sait de la nature et de l'étendue de l'incident lié à la cybersécurité, sur ce qu'il a fait pour rétablir la situation et réagir, et sur les mesures supplémentaires prévues.

[2] Si l'ARSF a besoin de renseignements supplémentaires concernant un incident, conformément à l'article 29 de la *Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs hypothécaires et les administrateurs d'hypothèques*, l'ARSF a le pouvoir d'exiger des titulaires de permis qu'ils fournissent au directeur général les renseignements et documents supplémentaires que ce dernier peut demander, et qu'ils le fassent de la manière et dans les délais prescrits par le directeur général.

**Phase 2 :** Au fur et à mesure que des renseignements plus complets sont disponibles, réception de mises à jour régulières de la part du titulaire de permis sur l'étendue ou les conséquences de l'incident sur ses clients et ses services. Les renseignements demandés dépendent de la nature de l'incident. Par exemple, dans le cas d'une atteinte de données, l'ARSF cherchera à comprendre clairement la nature et l'étendue de l'atteinte et les risques qu'elle présente pour les renseignements des clients.

**Phase 3 :** Réception par l'ARSF du plan du titulaire de permis visant à éviter tout incident semblable lié à la cybersécurité à l'avenir.

Le niveau et la fréquence du dialogue entre l'ARSF et le titulaire de permis dépendent de la nature et des conséquences de l'incident lié à la cybersécurité et tiennent compte des ressources dont le titulaire de permis a besoin pour répondre à l'incident.

# Date d'entrée en vigueur et examen futur

La présente ligne directrice entre en vigueur le 18 août 2022 et sera révisée au plus tard le 18 août 2025.

# À propos de cette ligne directrice

Le présent document est conforme au Cadre de lignes directrices de l'ARSF. En tant que ligne directrice en matière d'information, il décrit le point de vue de l'ARSF sur certains sujets sans créer de nouvelles obligations en matière de conformité pour les personnes réglementées.

# Références

- Principes de préparation à la cybersécurité du CCARCH
- Code de conduite du CCARCH
- Ligne directrice sur la gestion des risques liés aux technologies de l'information de l'ARSF[3]

**Date d'entrée en vigueur :** 18 août 2022

**Dernière mise à jour :** 12 avril 2024

[3] Ligne directrice sur la gestion des risques liés aux TI de l'ARSF publiée le 1er avril 2024.