

10 juillet 2025

**Guide d'application et de mise en œuvre**

# Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit

## Table des matières

1. Introduction .....	2
2. Objectif du guide .....	2
3. Organisations visées par le Règlement.....	3
4. Politique de gestion des Incidents .....	3
5. Procédures et mécanismes permettant de détecter, d'évaluer et de répondre aux Incidents .....	4
6. Signalement des Incidents .....	5
7. Registre des Incidents .....	6
8. Processus de signalement à l'AMF .....	9
9. Assistance.....	10

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2025

ISBN 978-2-555-01706-1

## 1. Introduction

L'encadrement de la gestion des incidents de sécurité de l'information (Incidents) par l'Autorité des marchés financiers (AMF) découle de l'obligation légale s'appliquant aux institutions financières (IF)<sup>1</sup> et aux agents d'évaluation du crédit (AEC) de suivre des pratiques de gestion saine et prudente<sup>2</sup>.

Établi sur la base de cette obligation, le *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit*<sup>3</sup> (Règlement) définit ce qu'est un Incident. Il énonce également les obligations des organisations visées par le Règlement en matière de signalement d'Incidents à l'AMF. La définition d'Incident est la base des obligations prévues au Règlement.



**Un Incident se définit comme étant « une atteinte<sup>4</sup> à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent »<sup>5</sup>.**

L'AMF a établi des lignes directrices pour informer les IF et les AEC des mesures qui, de son avis, peuvent être prises pour satisfaire aux obligations qui leur incombent en fonction des lois qui leur sont applicables. Ainsi, l'encadrement de la gestion d'un Incident se compose d'obligations réglementaires et d'attentes formulées dans les différentes lignes directrices.

Pour un rappel des attentes de l'AMF en matière de gestion d'Incidents, consultez les lignes directrices suivantes :

### Pour les fondements :

- [Ligne directrice sur la gouvernance](#);
- [Ligne directrice sur la gestion intégrée des risques](#);
- [Ligne directrice sur la conformité](#).

### Pour les attentes plus spécifiques :

- [Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications](#);
- [Ligne directrice sur la gestion du risque opérationnel](#);
- [Ligne directrice sur la gestion de la continuité des activités](#);
- [Ligne directrice applicable aux agents d'évaluation du crédit](#).

## 2. Objectif du guide

L'AMF a élaboré ce guide afin d'accompagner les organisations visées par le Règlement dans sa mise en œuvre et son application. Il apporte entre autres des précisions sur la politique de gestion des Incidents à élaborer, incluant

---

<sup>1</sup> Article 485 de la *Loi sur les assureurs*, RLRQ, c. A-32.1, article 601.1 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, paragraphe u de l'article 43 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, article 277 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02.

<sup>2</sup> Articles 47 et 66 de la *Loi sur les agents d'évaluation du crédit*, RLRQ, c.A-8.2. Dans le cas des agents d'évaluation du crédit, il est question de l'obligation de suivre des pratiques de gestion appropriées assurant le respect des droits conférés par la loi.

<sup>3</sup> A.M. 2024-13, 2024, G.O. II, 6381, [Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit](#)

<sup>4</sup> Le terme « atteinte » réfère à tout événement qui peut compromettre ou qui compromet la disponibilité, l'intégrité ou la confidentialité des systèmes d'information ou des informations qu'ils contiennent.

<sup>5</sup> Article 2 du Règlement.

les éléments à y intégrer, les procédures et mécanismes à mettre en place permettant de détecter, d'évaluer et de répondre aux Incidents, le contenu du registre des Incidents ainsi que le processus de signalement des Incidents à l'AMF.

À noter que le guide évoluera en continu en fonction des bonnes pratiques du domaine, de l'expérience acquise et des besoins des parties prenantes.

### 3. Organisations visées par le Règlement

Les organisations visées par le Règlement sont les assureurs autorisés, les fédérations de sociétés mutuelles, les fédérations de caisses ainsi que les caisses qui ne sont pas membres d'une fédération<sup>6</sup>, les institutions de dépôts autorisées, les sociétés de fiducie autorisées et les agents d'évaluation du crédit désignés par l'AMF (collectivement désignées par le terme « Organisations »).

À noter qu'une fédération de caisses est responsable du respect des obligations prévues au Règlement, notamment l'obligation d'établir et de mettre en œuvre une politique de gestion des Incidents à l'égard des caisses qui en sont membres et d'aviser l'AMF en cas d'Incident.

Dans le cas de sociétés mutuelles, chacune d'entre elles est responsable d'établir et de mettre en place une politique de gestion des Incidents et de signaler ceux-ci à l'AMF. Une fédération de sociétés mutuelles est également tenue de respecter les obligations réglementaires au même titre que les sociétés mutuelles.

Un assureur autorisé qui est une union réciproque ou un organisme d'autoréglementation n'est pas visé par le Règlement.

### 4. Politique de gestion des Incidents

Le Règlement prévoit l'obligation pour les Organisations d'établir et de mettre en œuvre une politique de gestion des Incidents. Ainsi, à l'instar des autres types de politiques, celle sur la gestion des incidents peut prendre différentes formes, c'est-à-dire qu'elle peut être spécifique ou faire partie intégrante d'une autre politique, telle qu'une politique sur la sécurité de l'information.

La politique devrait être constituée de tous les attributs propres à celle-ci et contenir notamment une description claire des rôles et responsabilités. À cet effet, les bonnes pratiques prévoient qu'une politique devrait être élaborée et révisée périodiquement par la haute direction et être approuvée par le conseil d'administration.

La politique de gestion des incidents doit minimalement mentionner les documents officiels décrivant les procédures et les mécanismes de l'Organisation qui lui permettent de détecter, d'évaluer et de répondre aux Incidents. Si les pratiques de détection, d'évaluation et de réponse aux incidents se basent sur des standards, des normes ou autres documents techniques de sources reconnues, ces derniers devraient être mentionnés à la politique.

Le Règlement étant construit sur la base de principes, les Organisations ont la flexibilité de déterminer le contenu de leur politique ainsi que son opérationnalisation.

---

<sup>6</sup> *Loi sur les coopératives de services financiers*, RLRQ, c. 67.2

## 5. Procédures et mécanismes permettant de détecter, d'évaluer et de répondre aux Incidents

L'AMF encourage les Organisations à s'inspirer des publications d'organismes nationaux et internationaux, comme l'Organisation internationale de normalisation (ISO)<sup>7</sup>, l'Information Systems Audit and Control Association (ISACA), le National Institute of Standards and Technology (NIST) ou encore le Control Objectives for Information and Related Technology (COBIT) pour développer leurs mécanismes et procédures. Ces organismes recommandent la mise en place de plusieurs bonnes pratiques qui contribuent à une saine gestion des Incidents.

Afin de s'assurer que la détection, l'évaluation et la réponse aux Incidents sont faites de manière cohérente et objective, les organismes nommés précédemment ont identifié de bonnes pratiques qui pourraient être mises en place par les Organisations. En voici des exemples :

- Catégoriser les Incidents en fonction de critères comme le type d'événement et les causes.
- Classifier les Incidents afin de définir le traitement et le niveau d'escalade requis.
- Utiliser des cotes prédéfinies aux fins d'établissement de la sévérité d'un Incident et de sa classification.
- S'assurer que l'ensemble des processus, procédures et mécanismes mis en place s'insèrent dans un processus global de gestion des Incidents.
- Établir des standards de documentation des Incidents afin de s'assurer d'une évaluation uniforme de ceux-ci.
- Mettre en place des mesures de contrôle et de supervision afin de s'assurer de gérer les Incidents de manière à atteindre les objectifs suivants :
  - Minimiser les préjudices subis;
  - Diminuer le risque de récurrence de l'Incident;
  - Signaler leur survenance.
- Mettre à jour et tester annuellement l'ensemble des mécanismes de détection et de réponse aux Incidents.
- Effectuer la collecte en continu d'informations dans les journaux des systèmes d'information afin d'enregistrer les activités des utilisateurs, les exceptions, les défaillances des systèmes et autres événements liés à la sécurité de l'information.
- Vérifier et tenir à jour les journaux des systèmes d'information.
- Obtenir des informations sur les vulnérabilités techniques des systèmes d'information en temps opportun.



**L'exposition de l'Organisation à ces vulnérabilités devrait être évaluée et les mesures appropriées devraient être prises pour traiter tous les risques associés.**

- Demander aux employés et aux tierces parties qui utilisent les systèmes d'information et les services de technologies de l'information et des communications de l'Organisation de signaler toute faiblesse observée ou suspectée en matière de sécurité de l'information dans les systèmes ou services.
- Obtenir l'assurance raisonnable, avant d'entrer en relation d'affaires avec un tiers, que ce dernier a des procédures et des contrôles en place pour assurer une saine gestion de ses Incidents.

---

<sup>7</sup> Voir notamment la norme ISO 27035

## 6. Signalement des Incidents

### Signalement aux dirigeants et gestionnaires

L'Organisation doit prévoir à sa politique des critères de signalement (escalade) internes aux différents paliers hiérarchiques, incluant les dirigeants ou les gestionnaires<sup>8</sup>.

L'Organisation doit aussi prévoir un signalement à l'AMF de même qu'à toute partie prenante, comme les clients, les tiers, les consommateurs et les autres organismes de réglementation<sup>9</sup>, et ce, en fonction des différentes obligations qui lui sont applicables.

Le délai pour effectuer le signalement et la méthode de signalement devraient être mentionnés à la politique. Dans l'établissement des différents signalements, l'Organisation doit aussi prendre en considération l'Incident qui survient chez un tiers à qui elle a confié l'exercice de toute partie d'une activité, dans la mesure où l'Incident affecte l'activité qui lui a été confiée.

Dans l'établissement des critères de signalement des Incidents, les bonnes pratiques recommandent de prendre en considération :

- la catégorisation;
- la sévérité;
- la classification.

La **catégorisation** permet de regrouper les Incidents dans le but d'en faciliter la gestion. Elle se base sur la nature de l'Incident, notamment :

- le type d'Incident, c'est-à-dire l'événement (vol de données, panne, etc.); ou
- les causes de l'Incident (cyberattaque, erreur humaine, etc.).

La **sévérité** d'un Incident indique l'importance et l'urgence que l'Organisation accorde à la maîtrise et la clôture (résolution) de l'Incident. Les critères utilisés pour déterminer la sévérité devraient notamment tenir compte :

- du temps prévu pour que les opérations reviennent en mode normal;
- de l'impact sur les clients;
- de l'ampleur des impacts confirmés ou prévus de l'Incident sur les opérations de l'Organisation, comme les impacts financiers, de réputation ou réglementaires;



**L'ampleur des impacts peut être évaluée en tenant compte notamment des données suivantes : les renseignements personnels, les actifs informationnels ou encore les utilisateurs affectés par l'Incident.**

- du moment de la survenance de l'Incident et du délai estimé pour sa clôture (résolution).

<sup>8</sup> L'utilisation des termes « dirigeants » et « gestionnaires » est basée sur la terminologie des lois sur lesquelles le Règlement s'appuie. Ainsi, dans le cas d'une caisse ou d'une fédération de caisses, il est question de « gestionnaires », tandis que pour les autres Organisations, le terme « dirigeants » est utilisé. Dans les deux cas, le terme fait référence à la haute direction de l'Organisation.

<sup>9</sup> Par exemple le Bureau du surintendant des institutions financières.

La **classification** vise à qualifier l'Incident afin de confirmer son statut et d'en prioriser la gestion. Elle doit prendre en considération l'ensemble des informations obtenues, dont :

- la catégorisation (type, cause);
- la sévérité;
- la gravité des impacts pour l'Organisation, les clients et le système financier;
- tout autre élément pertinent.

## Personne responsable de la gestion des Incidents

L'Organisation doit prévoir à sa politique la nomination d'une personne responsable de surveiller la gestion et le signalement des Incidents. Cette personne devrait voir à l'établissement et à la mise en œuvre de la politique dans l'Organisation.



**Une case pour désigner la personne responsable de la gestion des Incidents est prévue dans les services en ligne de l'AMF.**

La déclaration des Incidents à l'AMF relève du responsable de la gestion et du signalement des Incidents, mais ce dernier peut la déléguer à un autre intervenant.

En cas de doute quant à l'importance relative d'un événement ou d'un Incident, l'Organisation peut consulter son responsable des relations avec les institutions ou encore communiquer directement avec l'[AMF](#).

## Signalement à l'AMF par une Organisation faisant partie d'un groupe financier

Chaque Organisation visée par le règlement est responsable d'effectuer le signalement d'un Incident dans les services en ligne de l'AMF. Dans le cas où un Incident touche plusieurs Organisations membres d'un même groupe financier, il est possible de transmettre un seul signalement à l'AMF pour l'ensemble des Organisations membres du groupe financier visées par l'Incident.

Dans cette situation, l'Organisation signalante devra indiquer à la question 3 qui se trouve à la page 6 du formulaire que le signalement est fait pour l'ensemble des Organisations membres du groupe financier et indiquer le nom de toutes les Organisations faisant partie du groupe financier visées par l'Incident. Malgré ce qui précède, chaque Organisation demeure responsable de l'obligation de signalement et peut être tenue responsable d'un manquement dans le cas où le signalement n'est pas effectué conformément au Règlement, même si l'exécution du signalement est confiée à une Organisation membre du groupe financier au bénéfice de l'ensemble de ce groupe.

## 7. Registre des Incidents


Chaque Organisation doit tenir et mettre à jour un registre des Incidents. Les renseignements consignés au registre doivent être conservés d'une manière sécurisée et confidentielle, pendant une période de cinq ans à compter de la date du rapport de fin d'Incident.

Tous les renseignements relatifs au cycle de vie de la gestion des Incidents devraient être consignés au registre. Ceux-ci doivent être aussi complets que possible et permettre de soutenir les évaluations, les décisions et les mesures à prendre. Le registre devrait permettre de reproduire historiquement et fidèlement l'ensemble des renseignements recueillis et des interventions effectuées tout au long du cycle de vie de la gestion d'un Incident.

En plus d'être utilisés aux fins d'analyse, les renseignements consignés au registre peuvent permettre de faire ressortir des tendances en matière d'Incidents et ainsi contribuer à une saine gestion de l'ensemble des risques d'une organisation.

Les renseignements mentionnés ci-dessous doivent être minimalement consignés au registre.

Renseignements à consigner au registre	Précisions	Case correspondante du formulaire Web, lorsqu'applicable
<b>Date et heure de l'Incident</b>	<p>Viser la <b>détection</b> <u>et</u> l'<b>occurrence</b> de l'Incident.</p> <p>La détection est le moment où l'Incident a été rapporté pour la première fois dans l'Organisation, tandis que l'occurrence est le moment où l'Incident s'est produit (s'il est connu).</p>	<p><b>Moment où l'Incident a été rapporté</b> Page 3, question 7</p> <p><b>Moment où l'Incident s'est produit</b> Page 3, question 8</p>
<b>Localisation de l'Incident</b>	<p>Fait référence à l'origine de l'Incident, c'est-à-dire interne (employé) ou externe (consultant, tierce partie ou organisation malveillante reconnue)</p> <p>Dans le cas où l'origine est externe, le pays devrait être précisé.</p>	Page 3, question 12
<b>Nature de l'Incident</b>	La nature peut être déterminée par le type d'Incident (vol de données) ou encore la ou les causes de l'Incident (cyberattaque).	<p><b>Type principal de l'Incident</b> Page 3, question 5</p> <p><b>Cause(s) de l'Incident</b> Page 5, question 5</p>
<b>Description détaillée de l'Incident</b>	<p>La description devrait être exhaustive et, entre autres, comprendre les renseignements suivants :</p> <ul style="list-style-type: none"> <li>• la catégorisation;</li> <li>• la côte de sévérité;</li> <li>• la classification aux fins de traitement et de signalement;</li> <li>• les vulnérabilités identifiées;</li> <li>• les impacts en termes de disponibilité, d'intégrité et de confidentialité;</li> <li>• la nature des données affectées.</li> </ul> <p>Les informations suivantes peuvent également être intégrées :</p> <ul style="list-style-type: none"> <li>• l'appréciation quant à la récurrence potentielle d'un Incident de même nature;</li> <li>• les mesures prises pour la résolution des vulnérabilités identifiées;</li> <li>• les conclusions lors de la clôture de l'Incident.</li> </ul>	Page 3, question 4

Renseignements à consigner au registre	Précisions	Case correspondante du formulaire Web, lorsqu'applicable
<b>Préjudices engendrés par l'Incident</b>	Les critères pour établir les préjudices devraient notamment prendre en compte les services et les ressources affectées de même qu'une évaluation des impacts de l'Incident <sup>10</sup> .	
<b>Tiers concernés par l'Incident</b>	<p>Tout tiers impliqué dans l'Incident.</p> <p>Inclut les destinataires du signalement d'un Incident conformément à ce qui est prévu à la politique de l'Organisation.</p> <div data-bbox="493 684 599 800" style="display: inline-block; vertical-align: middle;">  </div> <p><b>Une bonne pratique est d'identifier le type de client touché par l'Incident et de donner une estimation de la volumétrie.</b></p>	<p><b>Intervenants internes ou externes liés</b> Page 3, question 12</p> <p><b>Clientèle affectée</b> Page 4, question 3</p> <p><b>Organisation(s) financière(s) ou non-financière(s) informée(s)</b> Page 3, question 15</p>
<b>Actions prises</b>	<p>Les actions prises comprennent :</p> <ul style="list-style-type: none"> <li>• les stratégies, procédures ou mesures d'atténuation mises en place afin de contrôler l'Incident et prévenir sa récurrence;</li> <li>• les communications envoyées conformément à la politique de l'Organisation;</li> <li>• la date et l'heure du ou des signalements.</li> </ul>	<p><b>Parties prenantes informées</b> Page 3, questions 13</p> <p>Date et heure du signalement</p> <p>Page 3, question 14</p> <p><b>Actions prises</b> Page 5, questions 1 à 4</p>
<b>Appréciation de l'Organisation quant à la récurrence potentielle de l'Incident</b>	<p>Évaluation de la probabilité que l'Incident se produise à nouveau.</p> <p>Cette évaluation peut être revue à la lumière de nouveaux renseignements sur l'Incident.</p> <p>Une bonne pratique est de documenter l'évolution de cette appréciation par l'Organisation.</p>	Page 6, question 2
<b>Actions prévues</b>	Il peut s'agir des mesures prises pour réduire la probabilité que de nouveaux Incidents de même nature se produisent à nouveau (si ces moyens ne sont pas encore mis en place).	Page 6, question 1

<sup>10</sup> Pour obtenir plus d'informations sur l'évaluation des impacts d'un Incident, consulter les pages 59 et suivantes du [Format for Incident Reporting Exchange \(FIRE\) : Final report 15 April 2025](#) du Financial Stability Board .

Renseignements à consigner au registre	Précisions	Case correspondante du formulaire Web, lorsqu'applicable
<b>Date de la maîtrise de l'Incident</b>	Date à laquelle l'Organisation a maîtrisé l'Incident et que les activités ont pu reprendre leur cours normal.  À noter que dans le cas d'un Incident impliquant des renseignements personnels, les activités ne sont pas toujours perturbées. Dans ce cas, on considère que l'Incident est maîtrisé lorsque la pratique ou le processus à l'origine de l'Incident a cessé ou a été corrigé.	Page 3, question 10
<b>Date de clôture de l'Incident</b>	Date à laquelle l'Incident est clos, c'est-à-dire que tous les plans d'action ont été réalisés.	Page 3, question 11

En plus des renseignements énoncés ci-dessus, le registre devrait contenir tous les renseignements sur l'Incident permettant à l'Organisation de faire un signalement complet à l'AMF.

## 8. Processus de signalement à l'AMF

Suivant ses critères de signalement internes aux différents paliers hiérarchiques, l'Organisation doit aviser l'AMF lorsqu'un Incident est signalé à ses dirigeants ou à ses gestionnaires. L'Organisation doit signaler les Incidents à l'AMF, par l'entremise des [services en ligne](#), au plus tard 24 heures après que le dirigeant, ou selon le cas, le gestionnaire a été avisé de la situation.

L'Organisation doit communiquer à l'AMF, au meilleur de sa connaissance, tout renseignement spécifié au formulaire de signalement jusqu'à ce l'Incident signalé soit maîtrisé et que le rapport de fin d'Incident ait été transmis.

Un Incident maîtrisé signifie généralement que les affaires ont repris leur cours normal sans nécessairement que la gestion de l'Incident soit totalement terminée.

Suivant le signalement initial à l'AMF d'un Incident, l'Organisation doit transmettre dans les [services en ligne](#) toute correction ou tout élément nouveau concernant l'Incident. Les signalements subséquents à l'AMF, pour chaque Incident, doivent être faits dans un délai n'excédant pas trois jours calendaires, et ce, même si aucun développement n'est apparu ou aucune information additionnelle n'a été découverte.

Tout au long du traitement d'un Incident et des signalements par l'entremise des services en ligne, l'AMF pourrait exiger des clarifications sur les renseignements rapportés. À ce titre, il sera possible pour les Organisations de joindre des documents complémentaires en annexe au formulaire de signalement de l'AMF.

L'ensemble des renseignements découlant du rapport doit être transmis à partir des champs prévus à cet effet dans le formulaire. Les renseignements ainsi qu'un rapport confirmant la maîtrise de l'Incident et la reprise normale des activités doivent être transmis dans un délai n'excédant pas 30 jours suivants la maîtrise de l'Incident. Il est aussi possible de transmettre dans les services en ligne, à la section « Documents supplémentaires », un rapport s'il contient des informations supplémentaires pertinentes qui n'ont pas déjà été communiquées.

## 9. Assistance

Pour obtenir de l'assistance dans l'utilisation des [services en ligne](#), les Organisations peuvent également trouver de l'information à la page [Comment s'inscrire aux services en ligne - Représentants et futurs professionnels | AMF](#) ou communiquer avec l'AMF au 1 877 525-0337.



En cas de doute au sujet de l'importance relative d'un Incident à signaler, les Organisations peuvent consulter la personne responsable de leur dossier à l'AMF ou encore [communiquer avec l'AMF](#).



Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

### Signalement des incidents de sécurité

1 2 3 4 5 6 7 8 9 Étape 1 de 9 : Information d'identification

*i* Ce formulaire permet aux organisations de signaler un incident de sécurité, conformément à l'obligation prévue au Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit.

#### Identification

**Information du client**

N° client  
Nom de l'entreprise  
**Adresse de correspondance**  
N° d'immeuble / Case postale  
Rue / Installation de livraison  
Municipalité  
Pays

Retour au menu Réinitialiser **Enregistrer et suivant >>>**

Les questions avec un \* sont obligatoires

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

### Signalement des incidents de sécurité

1 2 3 4 5 6 7 8 9 Étape 2 de 9 : Identification de la personne-ressource qui émet le signalement

*i* Cette personne sera le point de contact principal pour toute demande d'information spécifique provenant de l'Autorité en lien avec l'incident. L'Autorité communiquera avec cette personne jusqu'à la clôture / fermeture du signalement dans ses systèmes.  
\* Champ obligatoire

#### Identification de la personne-ressource qui émet le signalement

1. \* Nom de la personne qui émet le signalement d'incident Ariane Proulx ↻

2. \* Le titre (ou le rôle) de la personne qui émet le signalement ainsi que la direction ou le secteur de l'organisation auquel elle est rattachée Conseillère experte ↻

3. \* L'adresse courriel professionnelle à utiliser pour contacter la personne qui émet le signalement aproulx@abc.ca ↻

4. Adresse courriel supplémentaire (au besoin) pbastien@abc.ca ↻

5. \* Numéro de téléphone à utiliser pour joindre la personne qui émet le signalement 4188332215 ↻

Réinitialiser <<< Précédent **Enregistrer et suivant >>>**

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

### Signalement des incidents de sécurité

1 2 3 4 5 6 7 8 9 Étape 3 de 9 : Information sur l'incident de sécurité

**Champ obligatoire**

**Information sur l'incident de sécurité**

1. \* Numéro unique attribué à l'incident par votre organisation dans sa gestion interne des incidents

2. Numéros uniques (attribués par votre organisation) des autres incidents passés ou en cours dans votre organisation qui pourraient être liés à l'incident présentement signalé

3. \* Titre de l'incident, tel qu'il est défini dans le système de gestion d'incident de votre organisation

4. \* Veuillez décrire l'incident, en fournissant autant de détails que possible au moment présent (y compris les impacts en termes de disponibilité, intégrité et confidentialité de l'information et la nature des données affectées) et la façon dont il a été rapporté ou identifié au sein de votre organisation.

5. \* Veuillez identifier le type d'incident que vous signalez

- Interruption des activités, défaillance du système ou de l'exécution** Tout type d'incident qui perturbe la fourniture des activités, des fonctions ou des services d'une entité.
- Compromission (sans perturbation)** Violation de la sécurité d'un système d'information.
- Fuite de données** Compromission de la sécurité résultant en la destruction accidentelle ou illicite, la perte, l'altération, la divulgation non autorisée ou encore la transmission de données, stockées ou traitées.
- Vol, Fraude** Acte délibéré en vue d'obtenir un avantage financier non autorisé.
- Désordre de l'information** Diffusion d'informations fausses ou basées sur la réalité, qu'elles soient malveillantes ou non.
- Autre** (veuillez décrire le type d'incident selon la taxonomie utilisée par votre organisation).

6. La protection de renseignements personnels pourrait-elle avoir été compromise par l'incident?

7. Veuillez préciser le moment où l'incident a été détecté ou rapporté pour la première fois dans votre organisation (AAAA-MM-JJ HH:MM).

8. Veuillez préciser le moment, s'il est connu, où l'incident se serait produit (format AAAA-MM-JJ HH:MM).

9. \* Veuillez préciser le statut actuel de l'incident au sein de votre organisation :

**L'incident peut être « Ouvert » (toujours actif au sein de l'organisation), « Maltraité » (les activités ont repris leur cours normal) ou « Fermé ».**

*Notes: qu'à partir du moment où l'Autorité est avisée de la maîtrise de l'incident, vous avez 30 jours calendaires pour collecter et transmettre l'ensemble des informations requises et fermer celui-ci.*

*Pour qu'un incident puisse être fermé, tous les champs d'information obligatoires et requis par le règlement, incluant le rapport post-mortem, doivent avoir été remplis et transmis par le biais du présent formulaire. La fermeture de l'incident ne signifie pas que toutes les actions à venir décrites au rapport post-mortem ont été déployées. L'Autorité pourrait exiger une mise à jour sur l'état d'avancement du déploiement de ces mesures.*

10. Veuillez préciser la date et l'heure de la maîtrise de l'incident (format AAAA-MM-JJ HH:MM).   
*Précisez à quel moment les activités ont repris leur cours normal au sein de l'organisation.*

11. Veuillez préciser la date et l'heure de la clôture/fermeture de l'incident (format AAAA-MM-JJ HH:MM).   
*La clôture/fermeture d'un incident par votre organisation sous-entend que l'ensemble des renseignements exigés par ce formulaire de signalement ont été documentés adéquatement. L'Autorité pourrait communiquer avec la personne qui émet le présent signalement d'incident afin d'obtenir des précisions sur les informations transmises ou demander un supplément d'information à transmettre par l'entremise des champs « Information supplémentaire » ou « Documents supplémentaires » du présent formulaire.*

12. Veuillez identifier les intervenants internes ou externes connus qui sont liés à l'incident (ex. : employé ou consultant au sein de l'organisation, organisation malveillante reconnue), incluant leur localisation, si elle est connue, et préciser leurs actions qui ont mené à l'incident.  
*Il importe de préciser spécifiquement si une tierce partie faisant affaire avec votre organisation pourrait être mise en cause dans l'incident.*

Acteurs :

13. Veuillez indiquer les paliers supérieurs et autres parties prenantes de votre organisation mis au fait de l'incident selon les critères de signalement établis à votre politique de gestion des incidents (ex. : haute direction, conseil d'administration, CISO).

Niveau d'escalade interne impliqué dans la réponse à l'incident :

Directeur principal, Sécurité et gestion des édifices  
 VP - Sécurité et gestion des édifices  
 Directeur Principal - Gestion des TI  
 VP- TI

14. Veuillez préciser la date et l'heure auxquelles vous avez communiqué l'existence de cet incident à l'une ou l'autre des parties suivantes :

- Dirigeants ou, selon le cas, gestionnaires
- Tiers à qui votre organisation a confié l'exercice de toute partie d'une activité
- Organismes de réglementation
- Personne ou organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, ou, contractuellement, est chargé de dédommager le préjudice qui aurait pu être causé par cet incident
- Commission d'accès à l'information
- Clients ou consommateurs (l'heure est facultative dans ce cas)

Date et heure des signalements aux parties prenantes prévues au règlement (format AAAA-MM-JJ HH:MM) :

Directeur principal, Sécurité et gestion des édifices: 05/05/2025, 20:30  
 VP - Sécurité et gestion des édifices: 05/05/2025, 22:10  
 Directeur Principal - Gestion des TI: 05/05/2025, 20:30  
 VP- TI: 06/05/2025, 08:15

15. Veuillez nommer tout autre organisation financière ou non financière informée de cet incident (ex. : fournisseurs de services, spécialistes d'enquête, médias).

Organisations financières ou non financières informées :

SPCA  
 Gestion de la faune  
 AMF

Réinitialiser    Précédent    Enregistrer et suivant

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
 Autres demandes

**Signalement des incidents de sécurité**

1 2 3 4 5 6 7 8 9 Étape 4 de 9 : Description des répercussions ou des préjudices engendrés, estimés ou appréhendés de l'incident signalé

Champ obligatoire

Description des répercussions ou des préjudices engendrés, estimés ou appréhendés de l'incident signalé

1. Veuillez préciser la sévérité attribuée à l'incident signalé selon les critères établis dans la politique de votre organisation.

Sévère

La sévérité indique l'importance et l'urgence que vous accordez à la résolution de l'incident. Vous pouvez aussi joindre de l'information sur la façon dont vous établissez la sévérité dans les champs « Information supplémentaire » ou « Documents supplémentaires » du présent formulaire.

2. Veuillez préciser les services ou les secteurs d'activités de votre organisation affectés par l'incident signalé. Le type de service et de ressource, la nature de leur criticité pour l'organisation et le type de perturbation subie pourraient tous être détaillés dans cette section.

Tous les services à Montréal sont affectés, le site web est non fonctionnel donc nous pouvons présumer que toutes les entités sont touchées. Nous n'avons pas le portrait global à l'heure actuelle. D'autres informations seront fournies ultérieurement.

3. Veuillez décrire, si elles sont connues, la nature et la volumétrie des clientèles (notamment au Québec) et des transactions affectées par l'incident ainsi que leur répartition géographique.

Pas définitif au moment présent. Doit être évalué.

4. Veuillez spécifier la sévérité des impacts suivants :

Impacts financiers : Modérés  
 Impacts opérationnels : Majeurs  
 Impacts réputationnels : Majeurs  
 Impacts légaux ou réglementaires : Modérés

Réinitialiser    Précédent    Enregistrer et suivant



Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit

Autres demandes

## Signalement des incidents de sécurité

1 2 3 4 5 6 7 8 9 Étape 5 de 9 : Informations relatives aux actions entreprises (en cours ou à venir) en vue de maîtriser l'incident

Champ obligatoire

### Informations relatives aux actions entreprises (en cours ou à venir) en vue de maîtriser l'incident

1. Veuillez préciser le temps estimé d'ici à la maîtrise de l'incident

2. Nature et origine des réactions des diverses parties prenantes externes connues à ce jour

Non définies à l'heure actuelle

3. Nature et moment de diffusion de toutes les communications externes émises à ce jour (ex. : avis aux personnes affectées)

Courriels aux TI, VP, DP et Sécurité envoyés le 05/05/2025 à 20.30  
Appels à la Gestion de la Faune le 05/05/2025 à 22.45  
Communiqué de Presse en préparation pour les clients (en cours)

4. Actions entreprises pour contrôler l'incident  
Par exemple, les procédures et solutions intérimaires mises en place pour maîtriser l'incident.

Serveurs d'un autre Centre seront utilisés pour remettre le site web en fonction. En cours.



5. Cause de l'incident

Bien que plusieurs causes puissent être associées à un incident, veuillez indiquer la cause principale de l'incident. La cause est ce qui a permis à l'incident de se produire (vecteur ou technique d'attaque par exemple).

- **Conception ou mise à jour du processus** Conception ou mise en œuvre inadéquate des processus.
- **Erreur humaine** Défaillance de l'exécution.
- **Conception, développement et tests (systèmes)** Défaillances résultant d'une définition incorrecte ou inadéquate des exigences, d'un non-respect des exigences pendant le développement, d'erreurs de mise en œuvre ou de configuration et de tests inefficaces ou atypiques.
- **Contrôle des changements (systèmes)** Processus de modifications aux systèmes d'information ou à leur configuration inadéquat (autorisation, révision, rigueur).
- **Capacité et performance (systèmes)** Incapacité à gérer une charge ou un volume d'information donnée, à exécuter des instructions ou à traiter des informations selon des paramètres acceptables.
- **Obsolescence (systèmes)** Maintenance inadéquate ou insuffisante des composants du système d'information, ou de son fonctionnement au-delà de la durée de vie supportée.
- **Défaillance opérationnelle chez un tiers (excl. la sécurité)** Non-respect des attentes ou des obligations contractuelles pour la fourniture de services ou de biens.
- **Défaillance de la sécurité chez un tiers** Compromission, violation ou fuite de données qui affectent négativement les actifs de valeur pour l'institution.
- **Catastrophe naturelle** Événement ou phénomène naturel susceptible d'entraîner des impacts de différentes natures, entre autres matériels, des bris de services ou autres perturbations.
- **Déni de service (DoS)** Impossibilité, pour un usager, d'accéder à un service en ligne en raison d'une augmentation soudaine du nombre de requêtes effectuées auprès du serveur hébergeant ce service.
- **Vol d'identité** Obtention et utilisation non autorisée de données personnelles d'une manière qui implique une fraude ou une tromperie, généralement à des fins économiques.
- **Menace interne** Acte délégué d'un acteur interne visant à endommager, perturber ou obtenir un accès non autorisé à des actifs informationnels.
- **Malware** Logiciels conçus dans le but de causer des dommages, directement ou indirectement, à des entités ou à leurs systèmes d'information.
- **Manipulation physique, endommagement, vol et perte** Actions qui ont une incidence négative sur les actifs d'une entité dans l'environnement physique.
- **Rançongiciel** Logiciel malveillant utilisé pour commettre une extorsion en entravant l'utilisation d'un système d'information ou de ses informations.
- **Détournement de ressources** Exploitation des ressources des systèmes d'information pour accomplir des tâches qui exigent de la puissance de traitement, ce qui peut avoir une incidence sur la disponibilité du système et/ou des services hébergés.
- **Ingénierie sociale (y compris l'hameçonnage)** Terme général désignant le fait de tenter de tromper les gens pour qu'ils révèlent des informations ou effectuent certaines actions.
- **Pourriel** Utilisation abusive des systèmes de messagerie électronique pour envoyer sans discernement des messages en masse non sollicités.
- **Ciblage d'applications Web** Actions qui compromettent la cybersécurité d'une application ou d'un service Web.
- **Autre** (veuillez inscrire l'information ci-dessous).

Réinitialiser

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

**Signalement des incidents de sécurité** ?

1 2 3 4 5 6 7 8 9 Étape 6 de 9 : Autres informations

**Autres informations** ?

**1. Veuillez préciser les enseignements tirés de l'analyse de l'incident à la suite de sa maîtrise ainsi que les autres actions ou mesures correctives à venir, le cas échéant. Vous pouvez aussi utiliser les champs « Information supplémentaire » ou « Documents supplémentaires » du présent formulaire pour fournir des détails supplémentaires.**

*Les enseignements tirés et les activités correctives détaillent toutes les vulnérabilités et les actions à prendre pour y remédier. Les mesures correctives envisagées à venir et la date d'achèvement estimée de chaque mesure permettront de suivre les progrès et d'évaluer ensuite si les causes profondes ont été traitées de manière adéquate. L'Autorité pourrait exiger une mise à jour sur l'état d'avancement du déploiement de ces mesures.*

À définir.

**2. Veuillez préciser, à la suite de la maîtrise de l'incident au sein de votre organisation, votre évaluation de la récurrence potentielle de cet incident, en prenant en considération les enseignements tirés et les activités correctives prévues pour y remédier.**

À définir.

**3. Veuillez utiliser ce champ pour apporter un supplément d'information ou pour répondre à des demandes d'information supplémentaire émises par l'Autorité.**

Réinitialiser <<< Précédent **Enregistrer et suivant** >>>

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

**Signalement des incidents de sécurité** ?

1 2 3 4 5 6 7 8 9 Étape 7 de 9 : Pièces justificatives à fournir

**Pièces justificatives à fournir** ?

**Documents - Avis d'incident de sécurité**

Documents supportant la demande  Reçu  Papier  Électronique

Réinitialiser <<< Précédent **Enregistrer et suivant** >>>

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

### Signalement des incidents de sécurité ?

1 2 3 4 5 6 7 8 9 Étape 8 de 9 : Transmission

**i** Cette page de formulaire vous permet de transmettre votre demande à l'Autorité des marchés financiers. Veuillez lire la déclaration et confirmer l'exactitude des renseignements fournis en cochant la case prévue à cet effet.

Il est de bon usage d'imprimer votre demande pour fin de vérification avant transmission et pour en conserver une copie dans vos dossiers.

Lorsque votre demande est complétée et que vous avez confirmé l'exactitude des renseignements fournis, procédez à la soumission de votre demande au moyen du bouton « Transmettre ».

\* Champ obligatoire

**Déclaration aux renseignements fournis** ?

Je déclare que les renseignements contenus dans la présente demande sont véridiques.

**Avertissement** ?

Veillez vérifier attentivement votre demande. Lorsqu'elle sera soumise, il vous sera impossible de l'annuler ou de la modifier.

Réinitialiser ← Précédent Imprimer votre demande Transmettre

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

### Signalement des incidents de sécurité ?

1 2 3 4 5 6 7 8 9 Étape 9 de 9 : Confirmation de transmission

**Confirmation de transmission** ?

La demande a été soumise pour traitement.  
Si le type de demande le rend nécessaire, le client sera notifié par une communication personnalisée.

N° client: 2001720782  
N° de demande: 2530148503

Retour au menu Produire bons de numérisation Imprimer

Accueil Dossier client Qualification Certification Divulgations Institutions financières et agents de crédit  
Autres demandes

### Signalement des incidents de sécurité ?

\* Afficher les demandes

No demande	No incident	Titre	Statut	Créé le	Dernière MAJ	Échéance
2530148503	123456	Invasion de rats laveurs dans la chambre des serveurs	Ouvert	2025-06-11 12:03	2025-06-18 16:06	2025-06-21
2530148392	123-456	Quebec	Ouvert	2025-05-21 14:26	2025-05-21 15:08	2025-05-24
2530148389	AMF	Québec	Ouvert	2025-05-14 14:42	2025-05-14 14:42	
2530148296	45632	Quebec	Ouvert	2025-04-14 15:04	2025-04-14 15:04	2025-04-17
2530148295	2512411	Exemple 1	Ouvert	2025-04-14 11:40	2025-04-14 11:40	2025-04-17
2530148260	wervfs	wersfd	Ouvert	2025-04-10 10:00	2025-04-10 10:00	2025-04-09
2530148259	sdfas	sdfs	Maîtrisé	2025-04-10 09:59	2025-04-10 09:59	2025-04-11
2530148255	wefs	fweef	Ouvert	2025-04-08 15:21	2025-04-08 15:21	2025-04-07