Autorité des marchés financiers

Le 16 janvier 2025

Consultation sur le formulaire de signalement des incidents de sécurité de l'information

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 (A.M. 2024-13, G.O. II,6381)

Le tableau qui suit démontre les renseignements qui seront demandés lors du signalement d'un incident de sécurité de l'information effectué via les Services en ligne de l'Autorité. La colonne de gauche contient les renseignements à compléter alors que la colonne de droite contient les explications sur les renseignements demandés.

Les champs qui suivent servent à identifier l'organisation qui émet le signalement	**Description des renseignements demandés**
Nom légal (ou désignation généralement reconnue)	Cette information correspond à celle apparaissant au profil de votre organisation dans les Services en ligne (SEL) de l'Autorité.
N° d'identification légal unique	Cette information correspond à celle apparaissant au profil de votre organisation dans les Services en ligne (SEL) de l'Autorité.
Les champs qui suivent servent à identifier la personne-ressource qui émet le signalement	
Nom	Nom de la personne qui émet le signalement d'incident. Cette personne sera le point de contact principal pour toute demande d'information spécifique provenant de l'Autorité en lien avec l'incident. Champ String(100)
Titre et direction	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. Champ String(100)
Adresse(s) courriel	La ou les adresses courriel à utiliser pour contacter la personne qui émet le signalement. L'Autorité communiquera avec cette personne jusqu'à la clôture (ou fermeture) du signalement dans ses systèmes. Champ String(100)
N° de téléphone	Numéro de téléphone à utiliser pour joindre la personne qui émet le signalement. L'Autorité communiquera avec cette personne jusqu'à la clôture (ou fermeture) du signalement dans ses systèmes. Champ String(20)
Informations décrivant ce qui s'est ou qui se produit relatif au présent incident	

N° de référence unique de l'incident de l'organisation	Numéro unique attribué à l'incident par votre organisation dans sa gestion interne des incidents. Champ String(100)
N°s de référence d'incidents reliés	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. Champ String(200)
Titre de l'incident	Titre de l'incident tel qu'il est défini dans le système de gestion d'incidents de votre organisation. Champ String(200)
Description de l'incident	Veuillez décrire l'incident, en fournissant autant de détails que possible sur l'incident 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. Champ String(4000)
Type d'incident	Type principal de l'incident que vous signalez, selon la taxonomie suivante : • **Panne de système** Système qui ne peut répondre à une demande car il est indisponible, brisé ou hors de service. • **Accès non autorisé** Accès aux données, aux programmes, aux systèmes et aux supports de données par des personnes non autorisées, dû à la fois à des causes accidentelles et aux intentions malveillantes, ainsi que toute tentative accidentelle ou délibérée de pénétrer dans le système de sécurité. • **Attaque de force brute** Cyberattaque qui consiste à trouver un mot de passe ou une clé cryptographique en essayant systématiquement et successivement toutes les combinaisons possibles. • **Hameçonnage** Technique de fraude basée sur l'usurpation d'identité, qui consiste à envoyer massivement un message en se faisant passer pour une institution financière ou une entreprise commerciale de renom afin d'induire les destinataires en erreur et de les inciter à révéler des informations sensibles à leur insu. • **Rançongiciel** Logiciel malveillant qui permet de verrouiller un ordinateur ou d'en chiffrer les données, dans le but d'extorquer de l'argent à l'utilisateur. • **Erreur humaine** Erreur découlant d'une action humaine (ou d'une absence d'intervention) et pouvant produire un résultat non recherché. • **Fraude** Fait de s'approprier le bien d'autrui en usant de tromperie, ou de manœuvres frauduleuses. • **Vulnérabilité** Faiblesse d'un système informatique se traduisant par une incapacité partielle de celui-ci à faire face aux attaques ou aux intrusions informatiques. • **Erreur de système** Divergence entre une valeur ou une condition calculée, observée ou mesurée et la valeur ou la condition vraie, spécifique ou théoriquement correcte correspondante. • **Piratage psychologique** Méthode d'extorsion d'information sensible par laquelle un individu établit un faux lien de confiance avec sa victime afin qu'elle divulgue elle-même une information pouvant être utilisée à des fins malveillantes. • **Déni de service** 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'information** Un individu a subtilisé des informations, sans nécessairement mener une attaque cybernétique. • **Autres** (veuillez décrire le type d'incident selon la taxonomie utilisée par votre organisation) Champ Liste déroulante
Protection de renseignements personnels	La protection de renseignements personnels pourrait-elle avoir été compromise par l'incident rapporté? • Oui • Non • Incertain au moment présent Champ Booléen

Date et heure de la détection de l'incident	Le moment où l'incident a été détecté ou rapporté pour la première fois dans votre organisation. Champ DateTemps AAAA-MM-JJ HH:MM
Date et heure de l'occurrence de l'incident	Le moment, s'il est connu, où l'incident se serait produit. Champ DateTemps AAAA-MM-JJ HH:MM
Statut de l'incident	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), « Maîtrisé » (les activités ont repris leur cours normal) ou « Fermé ». Notez 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.
Date et heure de la maîtrise de l'incident	Veuillez préciser la date et l'heure de la maîtrise de l'incident. Notez qu'à partir de la maîtrise de l'incident, l'organisation a 30 jours pour collecter et transmettre l'ensemble des informations requises. Champ DateTemps AAAA-MM-JJ HH:MM Précisez à quel moment les activités ont repris leur cours normal au sein de l'organisation.
Date et heure de la clôture (ou fermeture) de l'incident	La clôture (ou 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. Champ DateTemps AAAA-MM-JJ HH:MM
Acteurs	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. Champ String(4000)
Niveau d'escalade interne impliqué dans la réponse à l'incident	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). Champ String(500)
Date et heure des signalements aux parties prenantes prévues au règlement	Veuillez préciser la date et l'heure auxquelles vous avez communiqué l'existence de cet incident aux parties prenantes suivantes : • Clients ou consommateurs • 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 Champ String(500)
Organismes ou autorités financières ou non financières informés	Veuillez nommer tout autre organisme financier ou non financier informé de cet incident (ex. : fournisseurs de services, spécialistes d'enquête, médias). Champ String(500)
Informations décrivant selon l'institution les répercussions ou préjudices engendrés, estimés ou appréhendés de l'incident signalé.	
Sévérité de l'incident	Veuillez préciser la sévérité attribuée à l'incident signalé selon les critères établis dans la politique de votre organisation. 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. Champ String(100)
Services et ressources affectés	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. Champ String(1000)
Clientèles affectées et volumétrie	Veuillez décrire, si elles sont connues, la nature et la volumétrie des clientèles (notamment au Québec) et des transactions mises en jeu dans l'incident ainsi que leur répartition géographique. Champ String(500)
Impacts financiers	• Inconnus • Faibles • Modérés • Importants • Majeurs Champ Booléen
Impacts opérationnels	• Inconnus • Faibles • Modérés • Importants • Majeurs Champ Booléen

Impacts réputationnels	• Inconnus • Faibles • Modérés • Importants • Majeurs Champ Booléen
Impacts légaux ou réglementaires	• Inconnus • Faibles • Modérés • Importants • Majeurs Champ Booléen
Informations relatives aux actions entreprises (en cours ou jusqu'à la clôture ou fermeture de l'incident) par l'institution pour en venir à maîtriser l'incident.	
Temps estimé pour maîtriser l'incident	Le temps estimé nécessaire pour maîtriser l'incident, à partir de la transmission du formulaire. Champ String(100)
Réactions du public ou d'autres parties prenantes	Nature et origine des réactions des diverses parties prenantes externes connues à ce jour. Champ String(1000)
Communications externes émises à ce jour	Nature et moment de diffusion de toutes les communications externes émises à ce jour (ex. : avis aux personnes affectées). Champ String(1000)
Actions entreprises pour contrôler l'incident	Par exemple, les procédures et solutions intérimaires mises en place pour maîtriser l'incident. Champ String(2000)
Causes de l'incident	La cause explique pourquoi l'incident a eu lieu. Elle peut fournir un aperçu précoce alors que l'incident est toujours en cours. Champ String(2000)

Autres informations	
Enseignements tirés et mesures correctives à venir	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. Champ String(2000)
Risques résiduels	Veuillez préciser, à la suite de la maîtrise de l'incident au sein de votre organisation, votre estimation du potentiel de récurrence de cet incident, en prenant en considération les enseignements tirés et les activités correctives prévues pour y remédier. Champ String(1000)
Information supplémentaire	Veuillez utiliser ce champ pour apporter un supplément d'information ou pour répondre à des demandes d'information supplémentaire émises par l'Autorité. Champ String(4000)
Documents supplémentaires	Veuillez utiliser la section suivante pour transmettre les documents qui ne peuvent être inclus ailleurs dans le présent formulaire.