Instructions

Titre	Formulaire Signalement d'un incident lié à la technologie ou à la cybersécurité du BSIF – Instructions détaillées
Date	15 janvier 2025
Sector	Banques Succursales de banques étrangères Sociétés d'assurance vie et de secours mutuels Sociétés des assurances multirisques Sociétés de fiducie et de prêts

Table des matières

Instructions

Conformément à notre préavis intitulé Signalement des incidents liés à la technologie et à la cybersécurité, les institutions doivent signaler les incidents liés à la technologie et à la cybersécurité au plus tard dans les 24 heures après qu'ils se sont produits. Le préavis est accompagné d'une liste des critères de signalement.

Lors du signalement initial des incidents actifs ou en cours, il faut au minimum remplir les champs obligatoires. Les autres champs peuvent être remplis et soumis au fur et à mesure que l'information devient disponible. Les champs

obligatoires sont marqués d'un astérisque (*). Pour les incidents réglés, donner le plus d'information possible.

Veuillez fournir les meilleures estimations possibles, notamment en ce qui a trait aux répercussions de l'incident sur le plan financier et la clientèle, et l'information n'a pas à être définitive au moment du signalement. Il est également possible de mettre à jour les renseignements fournis après l'incident, dans le cadre d'un rapport préparé après l'incident.

Jusqu'à ce que l'incident soit résolu, nous nous attendons à ce que les institutions fassent le point sur la situation, notamment au sujet des mesures et des plans de redressement à court et à long terme.

Selon la gravité de l'incident, ses conséquences et la vitesse à laquelle il se déroule, nous pouvons recommander les méthodes et la fréquence des mises à jour subséquentes.

Les institutions doivent transmettre leur formulaire Signalement d'un incident à la Division du risque lié aux technologies, à l'adresse TRD-DRT@osfi-bsif.gc.ca, et à leur chargé de surveillance.

Instructions pour les sections du formulaire Signalement d'un incident

Renseignements sur l'incident

Nom de l'institution	Inscrire la dénomination sociale de l'institution financière fédérale.
Nom ou identifiant de l'incident	Inscrire l'identificateur utilisé à l'interne par l'institution financière fédérale pour désigner l'incident. Par exemple : • INC000001 • CIRT-MAJ-001 • Cyberincident 2024-941 – prise de contrôle d'un compte
Type de rapport d'incident	Le signalement initial est le premier formulaire transmis par l'institution. Une fois le formulaire initial transmis, tous les formulaires suivants seront considérés comme des mises à jour. Pour les formulaires de mise à jour, le même nom ou identifiant d'incident peut être utilisé.
État de l'incident	Un incident actif est un incident en cours qui nécessite des mesures d'endiguement ou de rétablissement qui n'ont pas encore été mises en œuvre. Pour les incidents actifs, le champ de description de l'incident du formulaire doit comprendre le plus de renseignements possible afin de réduire les demandes d'information au minimum. Les incidents actifs doivent faire l'objet de mises à jour régulières jusqu'à ce qu'ils soient réglés et fermés. Un incident réglé est un incident entièrement résolu, pour lequel toutes les mesures nécessaires ont été prises afin d'en atténuer les conséquences et de rétablir les activités normales.
Date, heure et fuseau horaire de survenance de l'incident	La date et l'heure (y compris le fuseau horaire) réelles à laquelle l'incident est survenu, que ce soit dans les locaux de l'établissement ou ceux d'un tiers. Une fois la date sélectionnée, entrer l'heure et le fuseau horaire dans les champs prévus à cet effet. Noter que l'heure doit être saisie dans un format de 24 heures (JJ-MM-AAAA HH:mm).
Date, heure et fuseau horaire de détection de l'incident	La date et l'heure (y compris le fuseau horaire) réelles à laquelle l'incident a été détecté, que ce soit par l'institution ou par un tiers. Une fois la date sélectionnée, entrer l'heure et le fuseau horaire dans les champs prévus à cet effet. Noter que l'heure doit être saisie dans un format de 24 heures (JJ-MM-AAAA HH:mm).

Lieu de l'incident et secteurs d'activité touchés

Où l'incident s'est-il produit?	Sélectionner dans la liste déroulante l'option qui correspond le mieux au lieu où l'incident s'est produit. Si l'incident s'est produit : • dans une filiale ou chez un partenaire de coentreprise, choisir « Institution-filiale »; • dans une succursale étrangère d'une institution, choisir « Institution »; • chez un sous-traitant d'un tiers ou un tiers de quatrième niveau, choisir « Sous-traitant ». Si vous choisissez « Autre », donner des détails dans le champ suivant.
Tiers, sous-traitant ou autres renseignements	Si l'incident a débuté chez un tiers ou un sous-traitant, indiquer sa dénomination sociale complète.
Identification du secteur d'activité	Un secteur d'activité est un secteur d'affaires précis. Par exemple: • les services bancaires à la clientèle de détail; • le service des marchés financiers; • le service d'évaluation du crédit; • les services en ligne; • le service de paiement et règlement; • le service de gestion du patrimoine; • le service de tarification de l'assurance; • le service de règlement des demandes d'indemnisation; • le service des ressources humaines; • le service de réassurance; • le service de la comptabilité; • le service à la clientèle. Indiquer tous les secteurs d'activité et services touchés en les séparant par des virgules et en évitant les acronymes.
Site ou lieu touché	Si l'incident a des répercussions à plusieurs endroits, dresser la liste des lieux touchés ou décrire sa portée géographique. Indiquer également le nom des administrations ou des pays touchés. Indiquer les lieux ou emplacements touchés (par exemple, ville, province ou état, pays, à l'échelle mondiale).

Actifs technologiques touchés	Un actif technologique est un actif corporel (matériel, infrastructure, etc.) ou incorporel (logiciel, données, information, etc.) qui permet la prestation de services technologiques et doit être protégé. Indiquer le nom des actifs technologiques touchés et indiquer s'ils sont essentiels. Si le nom de l'actif n'indique pas sa fonction, donner une brève description. Développer tous les acronymes.

Détails de l’incident

Catégorie d’incident	Un incident technologique est une défaillance des actifs technologiques ou une perturbation de leur fonctionnement qui a une incidence sur les activités de l’entreprise ou les services qu’elle offre. Un cyberincident est un incident résultant d’un accès non autorisé ou d’une activité malveillante ciblant des systèmes d’information, des données ou des réseaux, généralement dans l’intention de voler, perturber ou endommager des actifs technologiques.
Conséquences de l’incident	Les conséquences de l’incident consistent en son résultat ou son incidence négative sur les actifs technologiques et les activités de l’organisation. Elles indiquent l’incidence de l’incident sur la confidentialité, la disponibilité ou l’intégrité des services, des systèmes ou des données. On parle de « compromission » lorsque l’incident cause la compromission de données, de systèmes ou d’utilisateurs en raison de la divulgation de données, de la prise de contrôle de comptes ou du fait que des entités non autorisées ont obtenu un accès privilégié à des systèmes, par exemple. On parle de « dégradation » lorsque les conséquences d’un incident font en sorte qu’un service ou une application fonctionne à capacité réduite, par exemple lorsque le temps de réponse aux demandes est prolongé ou qu’il y a des retards de traitement. On parle d’« interruption de service » lorsque l’incident fait en sorte qu’une fonction ou un service n’est plus offert ou est hors ligne.

Type d’incident	Le type d’incident décrit la façon dont il a été déterminé, selon les observations, qu’un actif technologique a été dégradé. Le type d’incident peut également indiquer le vecteur de menace ou la technique d’attaque utilisée par un auteur de menaces, comme l’hameçonnage ou les maliciels, pour entraîner les conséquences de l’incident (dégradation, interruption ou compromission). Sélectionner l’option la plus pertinente dans la liste qui figure en dessous. Prise de contrôle d’un compte Incident dans le cadre duquel une partie non autorisée accède au compte d’un utilisateur ou d’un client. Problème d’application Lacunes ou défaillances dans la couche d’applications logicielles causant des problèmes de rendement, des vulnérabilités ou d’autres problèmes opérationnels. Perte ou divulgation de données L’accès non autorisé à des données ou leur divulgation, utilisation abusive ou destruction, qui entraîne souvent une atteinte à la vie privée ou la perte de données essentielles. Déni de service Le fait qu’un service ou une application ne soit plus disponible en raison d’un important trafic provenant de sources malveillantes coordonnées et parfois multiples. Problème d’infrastructure Lorsque les défauts et les défaillances d’un système d’infrastructures technologiques sous-jacent nuisent à ses fonctionnalités opérationnelles. Par exemple, lorsque les défaillances de serveurs, de réseaux, de matériel, de systèmes d’exploitation, de la virtualisation, d’intergiciels, de bases de données et de centres de données causent une dégradation et une panne. Maliciel ou rançongiciel Incident dû à l’utilisation de logiciels malveillants comme des virus, des chevaux de Troie, des vers et des rançongiciels conçus pour endommager ou perturber des actifs technologiques, ou pour y obtenir un accès non autorisé. Hameçonnage Tentative de fraude, généralement par courriel, visant à amener des personnes à révéler des renseignements de nature délicate, comme des mots de passe ou des numéros de carte de crédit, en se faisant passer pour une entité digne de confiance. Accès non autorisé Lorsqu’une entité malveillante accède à un système ou à des données internes.

Niveau de gravité ou de priorité de l'incident	Le niveau de gravité ou de priorité représente le niveau de classification des incidents en fonction de leur incidence potentielle. Les institutions doivent utiliser leurs processus d'évaluation interne pour déterminer l'incidence potentielle de l'incident, le niveau de gravité 1, de priorité 1 ou de priorité critique étant le plus élevé. Si les catégories internes comportent plus de quatre niveaux, sélectionner une option aussi proche que possible du niveau attribué à l'interne.
Description de l'incident	La description de l'incident doit comprendre toute information supplémentaire qui n'est pas saisie dans les champs précédents et fournir plus de renseignements quant au contexte de l'incident, à sa détection, à ses répercussions, aux parties internes et externes touchées, aux mesures correctives prévues et aux leçons qui en ont été tirées. Les informations peuvent comprendre des détails sur l'incident, tels que : • la méthode de détection • impacts directs et indirects connus • les parties internes et externes touchées • les actions réalisées et en cours d'exécution • les délais estimés pour résoudre l'incident ou pour mettre en œuvre des améliorations ou des contrôles • toute solution de rechange prévue ou mise en œuvre pour les incidents actifs.
Non-respect de l'objectif de temps de reprise (OTR) ou de l'objectif de point de reprise (OPR)	L'OTR est le délai maximal accepté pour restaurer les systèmes, les services ou les données à la suite d'un incident. L'OPR est la quantité maximale de données dont la perte puisse être tolérée, mesurée dans le temps. Il définit le moment auquel les données doivent être restaurées après un incident. Si vous sélectionnez l'option « en cours d'évaluation » lors d'un signalement initial, veuillez confirmer si l'OTR ou l'OPR ont été atteints dans une mise à jour ultérieure.
Activation du plan de continuité des activités (PCA) ou du plan de reprise après sinistre (PRS)	Le PCA est une procédure permettant de maintenir les activités essentielles pendant et après un incident, une perturbation ou une crise. Le PRS est un ensemble de politiques et de procédures relatives à la restauration des systèmes et des données après une catastrophe ou un incident majeur. Si vous sélectionnez l'option « en cours d'évaluation » lors d'un signalement initial, veuillez confirmer si le PCA ou le PRS ont été activés dans une mise à jour ultérieure.

Étendue de l'incidence – prestation de services	Si l'incident a eu une incidence sur la capacité d'offrir des services, sélectionner le niveau d'incidence déterminé par l'institution dans la liste déroulante. Les niveaux d'incidence vont d'aucune à critique, en passant par faible, modérée, et élevée. Si l'incidence sur la prestation des services est en cours d'évaluation, indiquer le résultat de l'évaluation dans une mise à jour ultérieure.
Étendue de l'incidence – (perte de) information de nature délicate	Si l'incident comprend la perte d'information de nature délicate, sélectionner le niveau d'incidence déterminé par l'institution dans la liste déroulante. Les niveaux d'incidence, dans l'ordre d'importance, sont : aucune, faible, modéré, élevé, critique. Si l'incidence sur l'information de nature délicate est en cours d'évaluation, indiquer le résultat de l'évaluation dans une mise à jour ultérieure.
Étendue de l'incidence – perception médiatique ou publique	Décrire les perceptions, rapports ou énoncés issus des médias grand public ou des médias sociaux. Indiquer le niveau actuel du discours médiatique ou public résultant de l'incident.
Incidence financière ou risque financier estimatif (en dollars canadiens)	Représente le coût total estimatif de l'intervention et des mesures correctives en réponse à l'incident (y compris les mesures correctives visant les clients). Si l'incidence financière est en cours d'évaluation, indiquer le coût estimatif dans une mise à jour ultérieure.
Nombre estimatif d'utilisateurs, de clients ou de transactions touchés	Indiquer le nombre estimatif d'employés, de clients ou d'opérations touchés par l'incident.
Temps de reprise estimatif	Si l'incident est en cours ou toujours actif, fournir la meilleure estimation possible de la date et de l'heure auxquelles il sera ou devrait être réglé.
Durée de l'incident	Indiquer la durée totale des incidents réglés. Celle-ci doit être mesurée du moment où l'incident est survenu au retour aux activités normales. Indiquer la durée en jours, heures et minutes.
Récurrence de l'incident	Si l'incident est lié à un incident antérieur, fournir des références au ou aux incidents déjà signalés. Si le lien de récurrence de l'incident est en cours d'évaluation, veuillez fournir le résultat de l'évaluation dans une mise à jour ultérieure.

Cause profonde de l'incident	La cause profonde d'un incident est le facteur sous-jacent qui doit être pris en compte pour éviter que la chaîne d'événements qui a causé l'incident ne se reproduise. Si la cause profonde de l'incident est connue au moment de son signalement, sélectionner la cause appropriée. Entrer toute autre renseignement utile dans le champ Description de la cause profonde, dont : cause de l'incident, contrôles défaillants à l'origine de l'incident, améliorations prévues pour éviter que l'incident ne se produise, etc. Si la cause profonde est en cours d'évaluation, nous nous attendons à ce que les institutions fournissent des renseignements sur celle-ci dans le cadre de mises à jour ultérieures ou d'un rapport préparé après l'incident. Voici la liste des descriptions des causes profonde des incidents : Gestion de la capacité Problèmes découlant d'une surcharge des systèmes découlant de demandes des utilisateurs ou de limites des ressources de TI excessives ou non pertinentes (p. ex., mémoire, processeur, virtualisations, serveurs, stockage, etc.). Erreur de configuration Incidents résultant d'une configuration incorrecte ou inappropriée des actifs technologiques. Processus défaillant Problèmes découlant de procédures, d'étapes, d'instructions ou de flux de travail inadéquats ou inefficaces. Défaut de conception Problèmes découlant de lacunes ou de faiblesses dans la conception de l'architecture des solutions technologiques. Installations ou sécurité physique Incidents découlant d'un accès non autorisé ou d'une atteinte physique à des emplacements sécurisés (p. ex., centre de données, salles de serveurs, bureaux, lieux où se trouvent des actifs technologiques essentiels). Échec de redondance Incidents survenant lorsque les mécanismes de sauvegarde ou de redondance, comme le basculement vers un site auxiliaire, ne permettent pas d'assurer la continuité lorsque le fonctionnement du système est perturbé. Équipement défectueux Défaillances d'actifs technologiques dues à des composants matériels ou logiciels défectueux. Erreur humaine Incidents causés par des erreurs ou des oublis de la part de personnes qui utilisent les technologies. Catastrophe naturelle

Renseignements sur l'auteur de la cybermenace

Tactiques, techniques et procédures (TTP) de l'auteur de la menace (cyberincidents)	Les TTP décrivent le comportement d'un auteur de menaces. Les tactiques donnent une description du plus haut niveau du comportement des auteurs de menaces. Les techniques en donnent une description plus détaillée, et les procédures sont les étapes détaillées et réalisables, au niveau le plus bas. Indiquer les détails connus du comportement de l'auteur de la menace ainsi que les vulnérabilités exploitées.
Indicateurs de compromission – algorithme de hachage, URL, courriel, adresse IP, etc.	Les indicateurs de compromission sont essentiellement des preuves ou des traces d'activités ou de comportements malveillants qu'un auteur de menaces a laissées derrière lui. Indiquer tous les indicateurs connus, techniques ou non, ainsi que des références aux vulnérabilités exploitées, le cas échéant. Il peut s'agir d'actes inhabituels, d'adresses IP, d'URL, d'en-têtes de courriels ou de hachages de fichiers. Par exemple : • emplacement ou heure de connexion inhabituel ou inconnu; • hxxps://malicious.url.example/page.asp; • CVE-2024-01283; • adresse IPv4 ou IPv6; • badsender@malicious.domain[.]exemple; • 44d88612fea8a8f36de82e1278abb02f.

Avis internes et externes

Avis à la haute direction	Sélectionner une option dans la liste déroulante pour indiquer si la haute direction (cadres supérieurs, membres du conseil d'administration, etc.) a été avisée de l'incident. Si la haute direction a été avisée, sélectionner la date, l'heure et le fuseau horaire réelles de l'avis. Une fois la date sélectionnée, entrer l'heure et le fuseau dans le ou les champs prévus à cet effet. Noter que l'heure doit être saisie dans un format de 24 heures (JJ-MM-AAAA HH:mm).
Autres organismes ou agences de surveillance ou de réglementation avisés	Saisir le(s) nom(s) de la ou des organismes avisés dans le champ de texte libre.
Organismes de sécurité ou d'application de la loi avisés	Saisir le(s) nom(s) de la ou des entités avisées dans le champ de texte libre.
Fournisseurs de cyberassurance avisés ou demande de règlement	Sélectionner une option dans la liste déroulante pour indiquer si des fournisseurs d'assurance ou de cyberassurance ont été avisés ou si une demande de règlement a été présentée à la suite de l'incident.

Notes de bas de page

* Champ obligatoire