Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information

Institut canadien d'information sur la santé
Canadian Institute for Health Information

La production du présent document est rendue possible grâce à un apport financier de Santé Canada et des gouvernements provinciaux et territoriaux. Les opinions exprimées dans ce rapport ne représentent pas nécessairement celles de Santé Canada ou celles des gouvernements provinciaux et territoriaux.

À moins d'indication contraire, les données utilisées proviennent des provinces et territoires du Canada.

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
icis.ca
droitdauteur@icis.ca

Comment citer ce document :
Institut canadien d'information sur la santé. *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information*. Ottawa, ON : ICIS; 2025.

This publication is also available in English under the title *Privacy and Security Incident Management Protocol*.

Table des matières

Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information

1 Contexte

Ce protocole de l'Institut canadien d'information sur la santé (ICIS) traite des exigences concernant la détection, le signalement, le confinement, la notification, l'enquête et les mesures correctives en cas de violation de la vie privée ou de la sécurité de l'information. Les mêmes processus seront appliqués pour la détection, le signalement, le confinement, la notification, l'enquête et les mesures correctives dans le cas d'un événement qui constitue une violation réelle ou présumée de la vie privée ou encore une violation ou un incident lié à la sécurité de l'information.

Ce protocole vise tous les éléments d'actif informationnel de l'ICIS — notamment les renseignements personnels sur la santé (RPS), les renseignements personnels sur les travailleurs de la santé et sur les employés et d'autres renseignements personnels —, ainsi que les systèmes d'information. Tous les membres du personnel de l'ICIS sont tenus de suivre ce protocole, y compris les employés à temps plein et à temps partiel, les employés contractuels, les sous-traitants (notamment les tiers fournisseurs de services et fournisseurs de services électroniques), les personnes en détachement, les travailleurs temporaires et les étudiants.

Dans l'élaboration de ce protocole, l'ICIS a tenu compte des lignes directrices définies par la Commissaire à l'information et à la protection de la vie privée (CIPVP) de l'Ontario dans *Lignes directrices sur les interventions en cas d'atteinte à la vie privée dans le secteur de la santé*.

2 Définitions de « violation de la vie privée » et de « violation de la sécurité de l'information »

2.1 Au minimum, une violation de la vie privée inclut

- une collecte, une utilisation ou une divulgation de RPS non conformes à la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario ou à ses règlements ou à une autre loi applicable au Canada;
- un manquement aux politiques, procédures ou pratiques relatives au respect de la vie privée instaurées par l'ICIS, en lien avec les exigences du Manual for the *Review and Approval of Prescribed Persons and Prescribed Entities* de la CIPVP (le « Manuel ») mises en œuvre par l'ICIS;

- un manquement aux déclarations écrites, aux ententes de partage de données, aux ententes de recherche, aux ententes de confidentialité et aux ententes avec les tiers fournisseurs de services, en lien avec les exigences du Manuel mises en œuvre par l'ICIS; ou
- une situation où des RPS sont volés ou perdus ou sont recueillis, utilisés ou divulgués sans autorisation ou une situation où des enregistrements contenant des RPS sont reproduits, modifiés ou éliminés sans autorisation.

2.1.1 Certaines des situations ci-dessus peuvent constituer de simples incidents liés au respect de la vie privée, et non de réelles violations. Les violations présumées de la vie privée sont considérées comme étant des incidents liés au respect de la vie privée jusqu'à ce qu'il soit confirmé qu'elles sont de réelles violations.

2.2 Au minimum, une violation de la sécurité de l'information inclut un événement touchant les RPS qui

- compromet — de manière effective ou imminente — la confidentialité, l'intégrité ou la disponibilité de l'information de l'environnement informationnel;
- constitue une violation ou un risque imminent de violation de la LPRPS ou de ses règlements; ou
- constitue une violation ou un risque imminent de violation des modalités de toute entente écrite, d'autres obligations juridiques ou des politiques, procédures et pratiques de sécurité de l'information mises en œuvre par l'ICIS, en lien avec les exigences énoncées dans le Manuel.

2.2.1 Certaines des situations ci-dessus peuvent constituer de simples incidents liés à la sécurité de l'information, et non de réelles violations. Les violations de la sécurité de l'information sont considérées comme étant des incidents liés à la sécurité de l'information jusqu'à ce qu'il soit confirmé qu'elles sont de réelles violations.

3 Détection des violations de la vie privée et de la sécurité de l'information

3.1 Les membres du personnel de l'ICIS doivent signaler **immédiatement** une violation réelle ou présumée de la vie privée ou encore une violation ou un incident lié à la sécurité de l'information à l'adresse incident@icis.ca en mettant leur superviseur ou leur gestionnaire en copie conforme; ils n'ont pas besoin d'obtenir l'autorisation préalable de ces derniers. Le courriel acheminé à incident@icis.ca notifie l'incident au Secrétariat à la vie privée et aux services juridiques ainsi qu'à l'équipe de la sécurité de l'information, lesquels pourront ainsi commencer à en assurer la gestion.

3.2 Les notifications doivent inclure les renseignements suivants :

- le moment de la découverte de la violation ou de l'incident;
- la manière dont il a été découvert;
- l'emplacement;
- la cause (si elle est connue);
- les personnes concernées;
- tout autre renseignement pertinent, notamment toute mesure prise sur-le-champ en vue d'en confiner les effets.

3.3 Les violations réelles ou présumées de la vie privée peuvent également être découvertes par suite de vérifications du respect de la vie privée ou encore de plaintes ou de questions sur le respect de la vie privée.

3.4 Les violations ou incidents liés à la sécurité de l'information sont découverts par notification, notamment par les membres du personnel et les fournisseurs de services électroniques de l'ICIS, ainsi que par suite des vérifications ou de la surveillance requises de la part de l'ICIS, conformément aux documents suivants :

- la politique sur la maintenance des registres de contrôle et de vérification des systèmes;
- le manuel du Système de gestion de la sécurité de l'information.

3.5 Les violations réelles ou présumées de la vie privée et les violations ou incidents liés à la sécurité de l'information par suite d'une introduction par effraction dans les locaux de l'ICIS ou autre accès non autorisé à ces locaux doivent être signalés immédiatement à l'adresse incident@icis.ca.

4 Déterminer de l'occurrence d'une violation de la vie privée ou de la sécurité de l'information

4.1 Les personnes suivantes sont informées des événements signalés à incident@icis.ca :

- le chef de la sécurité de l'information (et son délégué);
- la chef de la protection des renseignements personnels et avocate générale (et son délégué).

4.2 Une réunion de l'équipe d'intervention en cas d'incident (l'équipe d'intervention) sera convoquée à la demande du chef de la sécurité de l'information et de la chef de la protection des renseignements personnels et avocate générale ou de leur délégué respectif. Y assisteront au minimum les membres du personnel suivants (ou leur délégué respectif) :

- un représentant de la direction de chaque section de l'ICIS touchée;
- un représentant de la direction de chaque division ou direction des Services et technologies de l'information touchée;
- un représentant du Centre de services (dans le cas d'un incident visant les applications ou les technologies de l'ICIS);
- tout autre membre du personnel qui devrait faire partie de l'équipe d'intervention.

Les membres du personnel sont tenus d'offrir une coopération immédiate et entière à l'équipe d'intervention et de prioriser les activités de gestion de l'incident.

4.3 Lorsqu'elle est notifiée d'une violation de la vie privée ou de la sécurité de l'information, l'équipe d'intervention doit déterminer

- s'il s'agit véritablement d'une violation de la vie privée ou de la sécurité de l'information et, le cas échéant, si des RPS ont été visés;
- la portée de la violation de la vie privée ou de la sécurité de l'information;
- si la violation touche la vie privée, la sécurité de l'information ou les deux.

4.4 Le degré de priorité d'une violation réelle ou présumée de la vie privée ou de la sécurité de l'information dépendra des risques et de facteurs tels que

- les répercussions potentielles de la violation;
- la capacité de récupération par suite de la violation réelle ou présumée;
- la mesure dans laquelle des RPS pourraient avoir été visés.

5 Notification d'une violation à la haute direction

5.1 L'équipe d'intervention notifiera aux personnes suivantes toute violation de la vie privée ou de la sécurité de l'information qui doit être déclarée en vertu des lois et règlements de l'autorité compétente ou des ententes de partage des données, y compris de la LPRPS :

- la vice-présidente, Services administratifs (ou son délégué);
- le dirigeant principal de l'information (ou son délégué);
- le président-directeur général (ou son délégué).

5.2 Les notifications seront envoyées le plus tôt possible. L'équipe d'intervention déterminera, au cas par cas, comment cette notification doit être fournie (p. ex. oralement ou par écrit) et la nature des informations à communiquer.

5.3 Au minimum, les notifications préciseront les informations suivantes :

- le moment de la découverte de la violation;
- le type de RPS en cause;
- l'état d'avancement de l'enquête;
- une description de la cause et des mesures de confinement;
- l'incidence sur les applications et les processus de l'ICIS;
- les autorités compétentes concernées;
- les obligations en matière de signalement et les exigences de communication;
- les mesures recommandées.

5.4 L'équipe d'intervention collaborera avec un représentant de la direction ou de la haute direction des Communications afin de coordonner la communication au sein de l'organisme et avec les intervenants externes selon les besoins.

5.5 Si l'on soupçonne que la violation réelle ou présumée pourrait entraîner une perturbation importante des activités nécessitant la mise en œuvre du plan de continuité des opérations, l'équipe d'intervention en informera la vice-présidente des Services administratifs, qui agit également à titre de présidente de l'équipe responsable de la continuité des opérations.

6 Confinement

6.1 Les membres du personnel de l'ICIS doivent **immédiatement** prendre les mesures de confinement appropriées. Il peut notamment s'agir de l'interruption ou de l'isolement de systèmes ou de services. Ces mesures pourraient devoir être prises en même temps que le signalement ou tout de suite après.

6.2 Lorsqu'elle procède à un confinement, l'équipe d'intervention doit veiller à

- prendre les mesures nécessaires dans les circonstances pour
  - protéger les RPS afin de prévenir tout autre vol, perte ou encore collecte, utilisation ou divulgation non autorisée;
  - protéger les enregistrements contenant des RPS afin de prévenir toute autre copie, modification ou élimination non autorisée;
- éviter que d'autres violations de la vie privée et de la sécurité de l'information se produisent de la même façon.

6.3 Au minimum, ces mesures de confinement doivent viser l'atteinte des objectifs suivants :

- Vérifier qu'aucun enregistrement contenant des RPS n'a été copié.
- Veiller à ce que les enregistrements contenant des RPS soient récupérés ou éliminés de façon sûre.
  - Lorsque les enregistrements contenant des RPS ont été éliminés de façon sûre, la date, l'heure et la méthode d'élimination sûre doivent être confirmées par écrit.
- Veiller à ce qu'il soit impossible de réaliser d'autres violations de la vie privée ou de la sécurité de l'information en utilisant la même méthode.
- Déterminer si la violation de la vie privée ou de la sécurité de l'information permettrait d'accéder sans autorisation à d'autres renseignements.
- Au besoin, tenir compte des autres mesures prises pour prévenir d'éventuelles violations de la vie privée ou de la sécurité de l'information.

6.4 L'équipe d'intervention doit

- déterminer le processus à suivre pour l'examen des mesures de confinement mises en œuvre, et déterminer si la violation de la vie privée ou de la sécurité de l'information a bien été confinée ou si d'autres mesures de confinement sont nécessaires;
- déterminer, au cas par cas, quels documents doivent être fournis à l'équipe d'intervention aux fins d'examen des mesures de confinement et ce qu'ils doivent contenir.

6.5 Lorsque d'autres mesures de confinement sont nécessaires, l'équipe d'intervention déterminera

- quels membres du personnel de l'ICIS sont responsables de définir les autres mesures de confinement;
- quels documents les membres du personnel doivent fournir à l'équipe d'intervention aux fins d'examen des mesures de confinement supplémentaires;
- le contenu des documents;
- le délai dont dispose le personnel pour fournir les documents à l'équipe d'intervention.

6.6 L'équipe d'intervention est la seule à pouvoir approuver le rétablissement des applications ou des services qui ont dû être interrompus.

6.7 Les résultats de l'examen des mesures de confinement initiales et supplémentaires consignés par l'équipe d'intervention, le cas échéant, compteront parmi les documents conservés dans CIHInow — le système des processus de l'ICIS maintenu par son équipe des Produits internes.

6.8 Si l'on soupçonne que les mesures de confinement requises pourraient entraîner une perturbation importante des activités et nécessiter la mise en œuvre du plan de continuité des opérations, l'équipe d'intervention en informera la vice-présidente des Services administratifs, qui agit également à titre de présidente de l'équipe responsable de la continuité des opérations.

7 Conservation des éléments de preuve

7.1 Il y a lieu de préserver les éléments de preuve pendant l'enquête et le confinement en cas de violation. En particulier, si la violation peut résulter d'actes malveillants, ou si on peut raisonnablement s'attendre à ce qu'une violation donne lieu à une poursuite en justice, l'ICIS fera appel à une firme indépendante d'experts judiciaires. Dans tous les cas, les membres du personnel de l'ICIS doivent tout mettre en œuvre pour que soient conservés les éléments de preuve tels que les fichiers de journalisation, les fichiers de cache, la copie bit à bit et les communications. Toutefois, si l'équipe d'intervention détermine que ces mesures de conservation font accroître les préjudices réels ou potentiels liés à la violation, en augmentant par exemple l'étendue ou la probabilité d'une violation de la vie privée ou de la sécurité de l'information, il est alors préférable de prioriser le confinement de la violation.

8 Notification de violation aux dépositaires ou à d'autres organismes

8.1 Les obligations de l'ICIS en matière de notification de violation sont définies dans un document interne.

8.2 L'ICIS doit informer, dès qu'il est raisonnablement possible de le faire, le dépositaire ou tout autre organisme ayant divulgué les RPS à l'ICIS lorsqu'on sait ou qu'on présume que ces renseignements ont été volés ou perdus ou encore recueillis, utilisés ou divulgués sans autorisation, et dans tous les cas où l'entente qui lie l'ICIS au dépositaire ou à l'autre organisme l'exige.

8.3 L'équipe d'intervention, en collaboration avec l'équipe des Communications et d'autres équipes au besoin, dirigera les communications internes et externes requises. Les membres du personnel de l'ICIS ne doivent communiquer **aucun** renseignement concernant un incident à l'externe, à moins d'en avoir reçu la directive de l'équipe d'intervention.

8.4 En l'espèce,

- la chef de la protection des renseignements personnels et avocate générale est responsable de notifier ou de demander qu'on notifie le dépositaire ou tout autre organisme;
- la notification peut être adressée verbalement et/ou par courriel, selon les circonstances;
- au minimum, le dépositaire ou tout autre organisme doit être informé des points suivants :
  - la portée de la violation de la vie privée ou de la sécurité de l'information;
  - le type de RPS en cause;
  - les mesures mises en place pour confiner la violation de la vie privée ou de la sécurité de l'information;
  - les autres mesures qui seront prises par suite de la violation de la vie privée ou de la sécurité de l'information, y compris l'enquête et les mesures correctives.

8.5 Si l'on soupçonne que la violation résulte d'un acte hostile, illégal, criminel ou de quelque autre façon illicite, la décision de communiquer avec les autorités et la responsabilité afférente incombent à la chef de la protection des renseignements personnels et avocate générale.

9 Notification de violation à la Commissaire à l'information et à la protection de la vie privée de l'Ontario (uniquement pour les renseignements personnels sur la santé de l'Ontario)

9.1 Dans les situations décrites aux paragraphes 6.3(1) et 18.3(1) de la LPRPS, dès qu'il est raisonnablement possible de le faire, l'ICIS doit notifier la CIPVP de toute violation de la vie privée ou de la sécurité de l'information, comme si l'ICIS était dépositaire.

9.2 La chef de la protection des renseignements et avocate générale est responsable de notifier la CIPVP ou toute autre personne ou organisation :

- La notification peut être adressée verbalement et/ou par courriel, selon les circonstances.
- Au minimum, la CIPVP ou toute autre personne ou organisation doit être informée des points suivants :
  - la portée de la violation de la vie privée ou de la sécurité de l'information;
  - le type de RPS en cause;
  - les mesures mises en place pour confiner la violation de la vie privée ou de la sécurité de l'information;
  - les autres mesures qui seront prises par suite de la violation de la vie privée ou de la sécurité de l'information, y compris l'enquête et les mesures correctives.

10 Notification de violation aux personnes visées

10.1 L'ICIS, en tant que collecteur secondaire de RPS, ne notifiera pas directement d'une violation de la vie privée ou de la sécurité de l'information les personnes concernées par les RPS. S'il y a lieu, la notification requise doit être adressée aux personnes par le ou les dépositaires en cause, à moins qu'une autre décision relative à la notification de violation aux personnes concernées ne soit approuvée par la CIPVP.

11 Enquête en cas de violation et recommandations

11.1 L'équipe d'intervention dirigera l'enquête sur la violation de la vie privée ou de la sécurité de l'information et nommera le ou les membres du personnel qui seront responsables de cette enquête.

11.2 Le ou les membres du personnel détermineront la nature et la portée de l'enquête, selon les circonstances (examens des documents, entrevues, visites des lieux, analyse judiciaire, inspections).

11.3 L'équipe d'intervention déterminera le processus que devront suivre le ou les membres du personnel de l'ICIS qui enquêtent sur la violation de la vie privée ou de la sécurité de l'information. Les points suivants feront partie du processus :

- les documents à remplir, à fournir et/ou à signer pour l'enquête, selon les circonstances;
- les informations que doivent contenir les documents;
- la désignation du ou des membres du personnel de l'ICIS chargés de remplir, de fournir et/ou de signer les documents.

11.4 Le ou les membres du personnel de l'ICIS transmettront ces documents à tous les membres de l'équipe d'intervention, avec copie conforme à incident@icis.ca.

11.5 L'équipe d'intervention devra

- charger d'autres membres du personnel de l'ICIS d'appliquer les mesures d'atténuation et toute autre recommandation pertinente, au besoin;
- définir les échéanciers pour la mise en place des mesures d'atténuation et des autres recommandations;
- effectuer un suivi et faire en sorte que les mesures d'atténuation et les autres recommandations soient mises en œuvre dans les délais fixés;
- évaluer les risques résiduels après la mise en œuvre.

11.6 Il incombe à l'équipe d'intervention de déterminer, dans la mesure du possible, la cause fondamentale de la violation, ainsi que les mesures correctives qui permettront de limiter le risque de récurrence. Ces mesures correctives peuvent être formulées dans le cadre de recommandations officielles intégrées au rapport de violation.

11.7 L'équipe d'intervention doit produire un rapport pour chacune des violations et peut le faire pour les incidents lorsqu'elle le juge approprié. Le rapport de violation doit être produit au terme de l'enquête sur la violation de la vie privée ou de la sécurité de l'information et déposé aux fins d'examen dès qu'il est raisonnablement possible de le faire, conformément à l'article 12.1.

11.7.1 Le modèle interne de rapport de violation de l'ICIS précise le niveau de détail requis lors de la communication des résultats de l'enquête.

12 Communication des résultats de l'enquête et des recommandations

12.1 L'équipe d'intervention enverra les rapports de violation, qui contiendront les résultats de l'enquête, les mesures d'atténuation et les autres recommandations, au Comité sur le respect de la vie privée, la confidentialité et la sécurité aux fins d'examen.

12.2 Selon les circonstances, les résultats de l'enquête peuvent être communiqués au président-directeur général de l'ICIS.

12.3 Tous les rapports de violation seront présentés au Conseil d'administration de l'ICIS. Ils indiqueront les résultats, les mesures d'atténuation et les autres recommandations pertinentes ainsi que l'état d'avancement de la mise en œuvre des mesures d'atténuation ou des recommandations.

12.4 Le Secrétariat à la vie privée et aux services juridiques consigne toutes les recommandations des rapports de violation dans le registre principal des plans d'action de l'ICIS, où elles feront l'objet d'une surveillance et d'un rapport à l'échelle organisationnelle. Ce rapport précisera qui sera chargé de mettre en œuvre les recommandations, d'établir l'échéancier de mise en œuvre de ces recommandations et de veiller à ce que la mise en œuvre respecte l'échéancier. Le responsable du plan d'action (soit le vice-président ou le directeur) doit consigner les mesures prises (ou prévues) pour mettre en œuvre les recommandations. De plus, chaque responsable du plan d'action devra régulièrement faire des présentations et des comptes rendus au Comité de la haute direction de l'ICIS. Des comptes rendus périodiques seront présentés jusqu'à ce que les recommandations aient toutes été mises en œuvre.

12.5 Le chef de la sécurité de l'information et/ou la chef de la protection des renseignements personnels et avocate générale peuvent, à leur discrétion, demander que certaines mesures de suivi soient mises en œuvre avant la clôture de l'incident. Le chef de la sécurité de l'information et/ou la chef de la protection des renseignements personnels et avocate générale détermineront les possibilités de formation et/ou de sensibilisation dans le cadre du processus de gestion des incidents et agiront en conséquence.

13 Suivi des violations de la vie privée et de la sécurité de l'information

13.1 Les documents ayant servi à la détection, au signalement, au confinement, à la notification, à l'enquête et à l'établissement des exigences en matière de mesures correctives en cas de violation de la vie privée et de la sécurité de l'information sont conservés dans CIHInow — le système des processus de l'ICIS maintenu par son équipe des Produits internes.

13.2 Le Secrétariat à la vie privée et aux services juridiques tiendra à jour un journal des violations réelles ou présumées de la vie privée comprenant les éléments suivants :

- la date de la violation réelle ou présumée de la vie privée;
- la date à laquelle la violation de la vie privée a été constatée ou soupçonnée;
- le type de RPS ayant fait l'objet de la violation de la vie privée, le cas échéant, de même que la nature et l'étendue de la violation réelle ou présumée de la vie privée;
- une description de la violation réelle ou présumée de la vie privée et des renseignements sur la personne qui l'a constatée;
- la cause de la violation réelle ou présumée de la vie privée;
- une mention indiquant si une personne non autorisée qui n'est pas un membre du personnel de l'ICIS ou un fournisseur de services électroniques est à l'origine de la violation réelle ou présumée de la vie privée, ainsi que le nom ou une description de cette personne, le cas échéant;
- la date à laquelle le président-directeur général ou le directeur exécutif (ou le détenteur d'un poste équivalent) et les membres de la haute direction ont été notifiés de la violation réelle ou présumée de la vie privée, le cas échéant;
- la date à laquelle la violation réelle ou présumée de la vie privée a été confinée et la description des mesures de confinement mises en œuvre;
- le nom du ou des membres du personnel de l'ICIS responsables du confinement pour la violation réelle ou présumée de la vie privée;
- la date de début de l'enquête;
- la date de fin de l'enquête;
- le nom du ou des membres de l'ICIS responsables de mener l'enquête;
- les résultats, les mesures d'atténuation et les autres recommandations pertinentes découlant de l'enquête;
- le nom du ou des membres du personnel de l'ICIS responsables de la mise en œuvre de chacune des recommandations;
- la mesure qui a été ou doit être prise pour mettre en œuvre chaque recommandation;
- la date à laquelle chaque recommandation a été ou doit être mise en œuvre;

- la date à laquelle le président-directeur général et les membres de la haute direction ont été informés des résultats, des mesures d'atténuation et des autres recommandations pertinentes découlant de l'enquête, le cas échéant;
- la date à laquelle le dépositaire ou tout autre organisme ayant divulgué à l'ICIS les RPS a été notifié, le cas échéant;
- la date à laquelle la CIPVP a été notifiée, le cas échéant;
- la date à laquelle les personnes ont été notifiées, le cas échéant.

13.3 L'équipe de la Sécurité de l'information tiendra à jour un journal des violations ou incidents liés à la sécurité de l'information comprenant les éléments suivants :

- la date de la violation ou de l'incident lié à la sécurité de l'information;
- la date à laquelle la violation ou l'incident lié à la sécurité de l'information a été constaté ou soupçonné;
- le type de RPS, le cas échéant, ayant fait l'objet de la violation ou de l'incident lié à la sécurité de l'information, de même que la nature et l'étendue de cette violation ou de cet incident;
- une description de la violation ou de l'incident lié à la sécurité de l'information et le nom de la personne qui l'a constaté;
- la cause de la violation ou de l'incident lié à la sécurité de l'information;
- une mention indiquant si une personne non autorisée qui n'est pas un membre du personnel de l'ICIS ou un fournisseur de services électroniques est à l'origine de la violation ou de l'incident lié à la sécurité de l'information, ainsi que le nom ou une description de cette personne, le cas échéant;
- la date à laquelle le président-directeur général et les membres de la haute direction ont été notifiés de la violation ou de l'incident lié à la sécurité de l'information, le cas échéant;
- la date à laquelle la violation ou l'incident lié à la sécurité de l'information a été confiné et la description des mesures de confinement mises en œuvre;
- le nom du ou des membres du personnel de l'ICIS responsables du confinement pour la violation ou l'incident lié à la sécurité de l'information;
- la date de début de l'enquête;
- la date de fin de l'enquête;
- les résultats, les mesures d'atténuation et toutes les autres recommandations pertinentes découlant de l'enquête;
- le ou les membres du personnel de l'ICIS responsables de la mise en œuvre de chacune des recommandations;
- la mesure qui a été ou doit être prise pour mettre en œuvre chaque recommandation;

- la date à laquelle chaque recommandation a été ou doit être mise en œuvre;
- la date à laquelle le président-directeur général et les membres de la haute direction ont été notifiés des résultats, des mesures d'atténuation et des autres recommandations pertinentes découlant de l'enquête, le cas échéant;
- la date à laquelle le dépositaire de l'information sur la santé ou tout autre organisme ayant divulgué à l'ICIS les RPS a été notifié, le cas échéant;
- la date à laquelle la CIPVP a été notifiée, le cas échéant;
- la date à laquelle les personnes ont été notifiées, le cas échéant.

14 Conformité, vérification et application

Le Code de conduite de l'ICIS définit le comportement éthique et professionnel attendu des employés en ce qui concerne les relations professionnelles, les renseignements (y compris les RPS) et le milieu de travail. Tous les employés de l'ICIS sont tenus de se conformer au code et à l'ensemble des politiques, procédures et pratiques de l'ICIS.

Les cas de non-conformité aux politiques en matière de respect de la vie privée et de sécurité sont traités conformément au *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information* de l'ICIS, en vertu duquel le personnel doit signaler tout incident ou toute violation à incident@icis.ca, ce qui comprend tout non-respect de cette politique.

La chef de la protection des renseignements personnels et avocate générale veille à garantir la conformité aux politiques, procédures et pratiques de respect de la vie privée. Le chef de la sécurité de l'information veille quant à lui à garantir la conformité à l'ensemble des politiques, procédures et pratiques de sécurité de l'information.

Tout manquement au code — y compris aux politiques, procédures et pratiques de respect de la vie privée et de sécurité — est signalé à la direction Personnel, Culture et Apprentissage, s'il y a lieu, et peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement, conformément aux lignes directrices sur les mesures disciplinaires pour les employés de l'ICIS.

La conformité est encadrée par la Politique de vérification du respect de la vie privée ou par le programme de vérification de la sécurité de l'information de l'ICIS, selon le cas.

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 511
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

70556-0325