Canada

Protégé une fois rempli

Formulaire de rapport d'atteintes substantielles à la vie privée en vertu de la *Loi sur la protection des renseignements personnels*

À l'usage des institutions gouvernementales du Canada qui signalent au Commissariat à la protection de la vie privée (le Commissariat) et au Secrétariat du Conseil du Trésor du Canada (SCT) des atteintes substantielles à la vie privée.

Qu'est-ce qu'une atteinte substantielle à la vie privée?

La *Politique sur la protection de la vie privée* définit une atteinte à la vie privée comme la création, la collecte, l'usage, la communication, la conservation ou le retrait inappropriée ou non autorisée de renseignements personnels ou accès inapproprié ou non autorisé aux renseignements personnels. Une atteinte substantielle est définie comme une atteinte à la vie privée qui pourrait vraisemblablement entraîner un risque réel de préjudice grave pour une personne.

Les préjudices graves comprennent :

- lésions corporelles;
- humiliation;
- dommage à la réputation et aux relations;
- perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles;
- perte financière;
- vol d'identité;
- effets négatifs sur un dossier de crédit;
- dommages ou perte de biens.

Qu'est-ce qu'un renseignement personnel?

La *Loi sur la protection des renseignements personnels* définit les renseignements personnels comme suit : « les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable ».

- les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille;
- les renseignements relatifs à son éducation, aux antécédents médicaux, criminels ou professionnels;
- les transactions financières;
- tout numéro d'identification;
- l'adresse, les empreintes digitales ou le groupe sanguin;
- les opinions ou points de vue personnels.

Une atteinte substantielle devrait-elle être signalée au Commissariat et au SCT?

Oui. Les atteintes substantielles à la vie privée doivent être signalées au Commissariat et au SCT.

Je suis une personne consciente de ou touchée par une atteinte à la vie privée. Dois-je utiliser ce formulaire?

Non. Si vous êtes un employé du gouvernement fédéral, veuillez communiquer avec le coordonnateur/la coordonnatrice de l'accès à l'information et protection des renseignements personnels (AIPRP) de votre

institution pour obtenir des conseils. Si vous souhaitez déposer une plainte concernant une atteinte à votre vie privée par une institution, veuillez consulter la section Signaler un problème du site Web du Commissariat.

Qui doit soumettre ce formulaire?

Le coordonnateur/la coordonnatrice de l'AIPRP de l'institution et ses bureaux constituent l'unique agent(e) de liaison lorsqu'il s'agit d'aviser le Commissariat et le SCT.

Devons-nous inclure des renseignements personnels dans ce formulaire?

Non. N'incluez pas les noms ou autres détails d'identification des employés ou des personnes touchées.

Dans combien de temps après une atteinte substantielle à la vie privée ce formulaire doit-il être soumis?

La *Politique sur la protection de la vie privée* exige que toute atteinte substantielle à la vie privée soit signalée au Commissariat et au SCT :

- Dès que possible après avoir déployé des efforts pour contenir, évaluer et atténuer l'atteinte;
- Au plus tard sept jours après que l'institution a déterminé que l'atteinte est substantielle.

Toutefois, les institutions peuvent aviser le Commissariat et le SCT de l'atteinte de manière informelle avant le délai de sept jours. Un avis précoce est recommandé si l'institution a besoin de conseils sur la manière de gérer l'atteinte.

Que peut-il se passer après qu'une atteinte a été signalée au Commissariat et au SCT?

Après avoir examiné le rapport d'atteinte, le Commissariat communiquera avec l'institution si des renseignements supplémentaires sont nécessaires ou afin d'offrir des conseils ou recommander des mesures correctives. Le SCT conseille les institutions sur la façon de gérer les atteintes substantielles à la vie privée qui touchent deux ou plusieurs institutions. Le SCT utilise également les informations sur les atteintes pour guider les politiques et les orientations.

Comment le Commissariat traitera-t-il les informations fournies par les institutions dans un rapport d'atteinte?

En vertu de la *Loi sur la protection des renseignements personnels*, le Commissariat a généralement l'obligation de maintenir la confidentialité des rapports d'atteintes à la vie privée soumis au commissaire à la protection de la vie privée. Il existe cependant quelques exceptions à cette obligation :

- Le Commissariat est assujetti aux lois sur l'accès à l'information et protection des renseignements personnels;
- Le Commissariat peut utiliser toute information, action ou inaction concernant les engagements pris en réponse à l'atteinte, dans une enquête potentielle ou comme base pour ouvrir une enquête en vertu de la *Loi sur la protection des renseignements personnels*.
- Le Commissariat peut aussi communiquer certaines informations limitées, par exemple pour confirmer qu'un rapport d'atteinte substantielle a été soumis, en cas de questions posées par le public ou les médias, tout en respectant les considérations de sécurité et les considérations légales.

Où puis-je obtenir de plus amples renseignements sur la réponse à une atteinte à la vie privée?

Pour obtenir de plus amples renseignements sur la réponse aux atteintes à la vie privée, veuillez consulter la page thématique Signaler une atteinte à la vie privée au sein de votre institution fédérale du Commissariat et la Trousse d'outils pour la gestion des atteintes à la vie privée du SCT.

Tous les champs doivent être remplis. Veuillez lire les instructions à la fin de ce formulaire afin de veiller à ce que toutes les sections soient remplies et exactes.

Il n'est pas nécessaire que tous les champs soient remplis dans les rapports modifiés ou mis à jour.

Est-ce le premier rapport lié à cet incident? (Sélectionner une option)

❍ Rapport original

❍ Rapport modifié ou mis à jour

Numéro de référence de l'institution :

Pour un rapport modifié ou mis à jour, indiquez le numéro de dossier du Commissariat :

A. Informations sur l'institution

A.1. Nom de l'institution

Sélectionnez le nom de l'institution dans la liste déroulante :

Nom de l'institution (s'il n'est pas disponible dans la liste déroulante) :

A.2 Coordonnées du coordonnateur/de la coordinatrice de l'accès à l'information et de la protection des renseignements personnels de l'institution

Nom :

Téléphone :

Poste téléphonique :

Courriel :

A.3 Coordonnées d'une personne-ressource qui peut répondre aux questions sur l'atteinte au nom de l'institution :

Sélectionner une option :

❍ Représentant interne ❍ Représentant externe (p. ex., un avocat.)

Nom :

Titre du poste :

Téléphone :

Poste téléphonique :

Courriel :

B. Informations sur l'atteinte à la vie privée

B.1. Personnes touchées

Nombre de personnes touchées par l'atteinte, si connu, ou nombre approximatif :

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

B.2. Chronologie de l'atteinte

Date de début (jj-mm-aaaa), ou date de début approximative, de l'atteinte :

Date (jj-mm-aaaa), ou date approximative, à laquelle l'institution a découvert l'atteinte :

Date (jj-mm-aaaa) à laquelle l'atteinte a été contenue, le cas échéant :

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

B.3. Type et cause de l'atteinte

Type d'atteinte (sélectionner **une** option qui vous convient le mieux dans la liste ci-dessous)

- ❍ Communication inappropriée et non autorisée
- ❍ Perte
- ❍ Vol
- ❍ Accès inapproprié et non autorisé
- ❍ Autre (p. ex., collecte excessive ou retrait accidentel de renseignements personnels.) (expliquer ci-dessous)

Cause de l'atteinte (sélectionner **une** option qui vous convient le mieux dans la liste ci-dessous. L'identification de la cause de l'atteinte peut nécessiter une consultation avec l'unité de sécurité de l'institution ou d'autres groupes internes.)

Cause externe – Cyberincident

- ❍ Attaque compromettant des informations d'identification : attaque par force brute
- ❍ Attaque compromettant des informations d'identification : attaque par pulvérisation de mot de passe ou attaque de table arc-en-ciel
- ❍ Attaque compromettant des informations d'identification : bourrage d'identifiant
- ❍ Autres attaques compromettant des informations d'identification
- ❍ Piratage
- ❍ Logiciel malveillant : rançongiciel
- ❍ Logiciel malveillant : détournement de formulaire
- ❍ Logiciel malveillant : injection

❍ Logiciel malveillant : cheval de Troie
❍ Logiciel malveillant : Ver informatique
❍ Autre attaque de maliciel
❍ Hameçonnage
❍ Autre cyberincident

Cause externe – Général

❍ Correspondance mal acheminée : courrier ordinaire
❍ Ingénierie sociale
❍ Vol
❍ Autre cause externe

Cause interne

❍ Accès aux renseignements sans privilèges d'accès
❍ Vulnérabilité de sécurité des applications
❍ Champ cci inutilisé
❍ Erreur de classification ou d'étiquetage
❍ Erreur de saisie de données
❍ Traitement des dossiers d'une manière non approuvée
❍ Élimination ou destruction inappropriée ou non autorisée
❍ Droits d'accès inappropriés fournis
❍ Perte ou égarement
❍ Correspondance mal acheminée : courriel
❍ Correspondance mal acheminée : courrier ordinaire
❍ Utilisation abusive des privilèges d'accès
❍ Utilisation abusive de connaissances privées ou confiées
❍ Vol
❍ Utilisation d'une solution de contournement ou d'un raccourci
❍ Utilisation de matériel ou d'appareil non approuvé ou inapproprié
❍ Utilisation de logiciels non approuvés ou inappropriés
❍ Autre cause interne

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

B.4. Description

Répondre aux questions suivantes. N'incluez aucun renseignement personnel ou information susceptible de compromettre la sécurité des systèmes gouvernementaux. Si des renseignements supplémentaires sont requis, le Commissariat ou le SCT communiquera avec l'institution.

1. Décrire comment et pourquoi l'atteinte s'est produite (inclure quelques détails techniques concernant l'atteinte, y compris une explication de la méthodologie en cas de cyberincident).

2. Identifier toutes les organisations et les tiers, le cas échéant, impliquées dans l'atteinte, y compris leurs rôles par rapport aux renseignements personnels en question. N'incluez pas les personnes touchées par l'atteinte, les parties qui ont obtenu un accès non autorisé ou les destinataires non autorisés ou les renseignements personnels.

3. Identifier l'emplacement physique ou géographique où l'atteinte s'est produite, si connu.

4. Décrire comment l'atteinte a été découverte.

5. Identifier tous les applications ou systèmes de la TI pertinents, le cas échéant.

6. Identifier les programmes ou services pertinents.

7. Décrire qui a pu avoir un accès non autorisé aux renseignements personnels (dans la mesure où cela est connu). Inclure une estimation du nombre de destinataires non autorisés.

8. Quelle est la relation entre les parties qui ont eu un accès non autorisé aux renseignements personnels, les destinataires probables des renseignements personnels et une ou plusieurs des personnes touchées?

B.5. Mesures de sécurité

Remarque : Pour remplir cette section, il peut être nécessaire de consulter l'unité de sécurité de l'institution ou d'autres groupes internes. N'incluez aucune information susceptible de compromettre la sécurité des systèmes gouvernementaux. Si des renseignements supplémentaires sont requis, le Commissariat ou le SCT communiquera avec l'institution.

Des mesures de sécurité étaient-elles en place au moment de l'atteinte pour empêcher qu'elle ne se produise? (Sélectionner une option)

❍ Oui ❍ Non ❍ Inconnu

Si oui, préciser la nature de ces mesures (cocher toutes les réponses applicables) :

❑ Mesures de protection administratives
❑ Mesures de protection physiques
❑ Mesures de protection techniques

Le cas échéant, quelles méthodes de protection physiques ou techniques étaient en place? (Cocher toutes les réponses qui s'appliquent.)

❑ Chiffrement
❑ Contrôle d'accès à la GI/TI (p. ex., mot de passe, identification de l'utilisateur, autorisations, protocole d'identification biométrique)
❑ Conteneur ou caisse sécurisé
❑ Authentification multifacteur

❑ Autre (préciser) :

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

B.6. Renseignements personnels

Sur qui portaient les renseignements personnels? (Cocher toutes les réponses qui s'appliquent.)

❑ Client ou bénéficiaire du service
❑ Employé fédéral
❑ Autre (préciser) :

❑ Inconnu (expliquer ci-dessous)

Dans la mesure où elles sont connues, quelles catégories de renseignements personnels l'atteinte a-t-elle compromises? (Sélectionner toutes les réponses applicables et indiquer les types)

Catégories	**Éléments de renseignements personnels** (n'inclure aucun renseignement personnel ou chiffre réel)
❑ Coordonnées	
❑ Information d'emploi	
❑ Information génétique	
❑ Information sur la santé	
❑ Information sur le compte	
❑ Numéro ou symbole d'identification attribués	
❑ Renseignements biométriques	
❑ Renseignements d'identification	
❑ Renseignements de sécurité ou de surveillance	
❑ Renseignements démographiques	
❑ Renseignements financiers et de crédit	
❑ Renseignements sur l'application de la loi et l'administration	
❑ Renseignements sur l'éducation	
❑ Renseignements sur l'emplacement	
❑ Renseignements transmis par le gouvernement	
❑ Autres renseignements indicatifs de préférences, d'opinions ou de comportements	
❑ Autres (préciser)	

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

Les renseignements faisant l'objet de l'atteinte sont-ils inclus dans un fichier de renseignements personnels (FRP) enregistré auprès du SCT? (Sélectionner une option)

- ❍ Oui
- ❍ Non : Un FRP n'est pas requis
- ❍ Non : Un FRP n'existe pas (p. ex., aucune autorité législative)
- ❍ Non : Un FRP est en attente d'enregistrement (EFVP/FRP envoyé au SCT pour approbation)
- ❍ Inconnu

Le cas échéant, indiquer les FRPs pour les informations faisant l'objet de l'atteinte. Lorsqu'il est connu, indiquer également le numéro d'enregistrement du SCT.

Titre du FRP de l'institution et numéro du FRP :

Numéro d'enregistrement du SCT :

B.7. Risques réels anticipés de préjudice grave pour un individu

Quels sont les risques réels anticipés de préjudice grave résultant de l'atteinte pour toute personne concernée? (Cocher toutes les réponses qui s'appliquent.)

- ❑ Lésions corporelles
- ❑ Humiliation
- ❑ Dommage à la réputation et aux relations
- ❑ Perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles
- ❑ Perte financière
- ❑ Vol d'identité
- ❑ Effets négatifs sur un dossier de crédit
- ❑ Dommages ou perte de biens

Expliquer pourquoi l'institution anticipe le risque réel de préjudice grave (n'inclure aucun renseignement personnel à moins qu'il ne soit essentiel pour expliquer le risque potentiel)

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

C. Avis

C.1. Avis aux personnes touchées

L'institution a-t-elle informé toutes les personnes touchées? (Répondre « oui » si l'avis est terminé ou prévu.) (Sélectionner une option)

❍ Oui ❍ Non

Date (jj-mm-aaaa) de début (ou prévue) de l'avis, le cas échéant :

Sélectionner une option

❍ Avis réel
❍ Avis planifié

Date (jj-mm-aaaa) de fin d'avis, le cas échéant :

Méthode d'avis utilisée ou prévue pour les personnes touchées (sélectionner une option) **:**

❍ Toutes les personnes touchées avisées directement
❍ Toutes les personnes touchées avisées indirectement
❍ Certaines personnes avisées directement et certaines personnes avisées seulement indirectement
❍ Certaines ou toutes les personnes touchées n'ont pas été avisées

Si l'institution a décidé de ne pas informer certaines ou toutes les personnes touchées, expliquer pourquoi.

C.2. Avis à d'autres organisations

Le cas échéant, quelles organisations d'application de la loi ont été informés de l'atteinte (services de police municipaux, provinciaux, territoriaux, fédéraux et internationaux)?

Nom de l'organisation/des organisations :

Date(s) (jj-mm-aaaa) d'avis :

Le cas échéant, énumérer toute autre organisation ou institution gouvernementale qui a été informée de l'atteinte. Par exemple, SPAC pour les atteintes impliquant des fournisseurs de services tiers ou la GRC pour la fraude (n'inclure aucune institution précédemment identifiée dans ce formulaire, comme le SCT).

Nom de l'organisation/les organisations :

Date(s) (jj-mm-aaaa) d'avis :

Commentaires supplémentaires (n'inclure aucun renseignement personnel)

D. Confinement et atténuation des atteintes à la vie privée

L'institution a-t-elle déterminé les destinataires non autorisés des informations? (Répondre « oui » s'il n'y a pas de destinataire non autorisé.) (Sélectionner une option)

❍ Oui ❍ Non ❍ Inconnu

Si oui, l'institution a-t-elle contacté les destinataires? (Répondre « oui » s'il n'y a pas de destinataire non autorisé.) (Sélectionner une option)

❍ Oui ❍ Non ❍ Inconnu

L'institution ou la personne touchée a-t-elle toujours accès aux informations compromises par l'atteinte (p. ex., une copie ou une sauvegarde)? (Sélectionner une option)

❍ Oui ❍ Non ❍ Inconnu

Décrire toute autre mesure prise ou prévue par l'institution pour atténuer le risque réel de préjudice grave pour les individus.

E. Prévention des atteintes à la vie privée

Décrire toutes les mesures prises ou prévues par l'institution pour réduire le risque qu'une atteinte similaire se produise à l'avenir

Remise du formulaire rempli

Soumettre ce formulaire au Commissariat et au SCT par **l'un** des moyens suivants :

❍ Par courriel:

Commissariat à la protection de la vie privée

notification@priv.gc.ca

Secrétariat du Conseil du Trésor

sec@tbs-sct.gc.ca **et** ippd-dpiprp@tbs-sct.gc.ca

❍ Par courrier postal ou en main propre :

Commissariat à la protection de la vie privée du Canada
Unité de réponse aux atteintes
Direction de la conformité, de l'accueil et de la résolution,
Commissariat à la protection de la vie privée du Canada
30, rue Victoria, 1er étage
Gatineau (QC) K1A 1H3

Secrétariat du Conseil du Trésor du Canada
Division de la protection de la vie privée et des données responsables,
Bureau de la dirigeante principale de l'information,
Secrétariat du Conseil du Trésor du Canada
90, rue Elgin, 4e étage
Ottawa (ON) K1A 0R5

Division des politiques sur la sécurité
Bureau de la dirigeante principale de l'information,
Secrétariat du Conseil du Trésor du Canada
90, rue Elgin, 4e étage
Ottawa (ON) K1A 0R5

Si vous avez besoin de plus amples renseignements sur les exigences en matière de signalement des atteintes en vertu de la *Directive sur les pratiques relatives à la protection de la vie privée*, veuillez communiquer avec la Division de la protection de la vie privée et des données responsables du SCT, en envoyant un courriel à ippd-dpiprp@tbs-sct.gc.ca.

Instructions pour remplir le formulaire de rapport d'atteinte substantielle en vertu de la *Loi sur la protection des renseignements personnels*

Tous les champs doivent être remplis et le formulaire doit être soumis au Commissariat et au SCT au plus tard sept jours après que l'institution a déterminé que l'atteinte est substantielle.

Une fois rempli, ce formulaire doit être marqué et sauvegardé en utilisant le niveau de classification approprié. Le formulaire doit être étiqueté « Protégé B » si des renseignements personnels sont inclus.

A.1 Nom de l'institution : Consulter le Registre des titres d'usage du Programme fédéral de l'image de marque.

A.2 Coordonnées d'une personne-ressource autre que le coordonnateur/la coordonnatrice de l'AIPRP : Entrer les coordonnées d'une personne autre que le coordonnateur/la coordonnatrice de l'AIPRP de l'institution qui peut répondre aux questions sur l'atteinte au nom de l'organisation. Les coordonnées du coordonnateur/de la coordonnatrice de l'AIPRP sont automatiquement ajoutées au fichier de rapport d'atteinte.

B.1. Nombre de personnes touchées par l'atteinte, si connu, ou nombre approximatif : Indiquer le nombre de personnes dont les renseignements personnels ont été ou pourraient avoir été compromis par l'atteinte. Si le nombre exact n'est pas connu, entrer le nombre approximatif et ajouter une note dans la section commentaires. Mettre à jour ces informations dans un rapport modifié si le nombre exact est connu.

Conseil : Pour obtenir de plus amples renseignements sur ce qui constitue des renseignements personnels, veuillez consulter le Survol de la *Loi sur la protection des renseignements personnels*.

B.2. Chronologie de l'atteinte : Indiquer la date à laquelle l'atteinte a commencé. En cas de doute, indiquer la date la plus rapprochée à laquelle l'atteinte aurait pu commencer. Par exemple, si un courrier mal acheminé est à l'origine de l'atteinte, saisir la date à laquelle le courrier a été envoyé.

« Quand l'institution a découvert l'atteinte » fait référence au moment où l'atteinte a été découverte pour la première fois, par exemple par un employé du BPR. Cette date de découverte peut être antérieure à la date à laquelle le coordonnateur/la coordonnatrice ministériel de l'AIPRP ou dirigeant principal de la sécurité a eu connaissance de l'atteinte.

Si l'atteinte est contenue, ce qui signifie que l'institution estime que les informations ne sont pas vulnérables à un accès, une communication ou un usage inapproprié ou non autorisé, ajouter la date à laquelle l'atteinte a été contenue. La date à laquelle l'atteinte a été contenue est indiquée comme « le cas échéant », car il se peut qu'il ne soit pas possible de contenir l'atteinte. Le cas échéant, les institutions peuvent soumettre un rapport mis à jour contenant des détails supplémentaires sur les mesures de confinement une fois leur mise en œuvre terminée.

Conseil : Pour obtenir de plus amples renseignements sur le confinement des atteintes, veuillez consulter la Trousse d'outils de gestion des atteintes à la vie privée du SCT.

B.3. Type et cause de l'atteinte : Ces informations sont importantes pour déterminer le risque réel de préjudice grave pour un individu et comment atténuer ce préjudice. Les institutions ne devraient indiquer qu'une seule cause d'atteinte, même si d'autres événements connexes aggravent le préjudice associé à l'atteinte. Tout événement secondaire ou aggravant lié à l'atteinte doit être indiqué dans la case « commentaires supplémentaires » afin que le contexte entier de l'atteinte puisse être compris.

Vous trouverez ci-dessous des explications sur les types d'atteintes utilisés dans ce formulaire. Ces types correspondent généralement à une terminologie connexe couramment utilisée dans les collectivités de la technologie de l'information (TI) et de la sécurité. D'autres types d'atteintes sont répertoriés dans la cinquième ligne et nécessitent un examen distinct quant à leur lien avec la terminologie de la TI/sécurité.

Type d'atteinte	Terminologie associée couramment utilisée dans les collectivités de la TI et de sécurité
Il y a **communication inappropriée et non autorisée** lorsque des renseignements personnels sont communiqués par l'institution (y compris par des tiers agissant dans le cadre d'une entente, d'un accord ou d'un contrat avec l'institution), intentionnellement ou non, à un destinataire qui n'a pas le « besoin de connaître. » Cette communication peut se produire à l'externe ou à l'intérieur d'une institution. Voici quelques exemples : • Affichage accidentel de renseignements personnels aux employés (p. ex., dans une présentation PowerPoint ou à la suite d'autorisations d'accès trop larges). • Dépersonnalisation insuffisante avant de transmettre des renseignements personnels. • Application incorrecte ou partielle de séparations ou de caviardages avant de communiquer des renseignements personnels. • Courriels non chiffrés et mal acheminés.	Cela correspond généralement au terme de la TI/sécurité : **Atteinte à la confidentialité**, qui inclut la communication inappropriée ou non autorisée d'informations.
La **perte** se produit lorsque l'institution (y compris les tiers agissant dans le cadre d'une entente, d'un accord ou d'un contrat avec l'institution) perd le contrôle des renseignements personnels en raison des actions de ses employés ou partenaires, de telle sorte que l'institution ne conserve plus l'accès aux renseignements personnels. Une perte peut entraîner l'accès ou le contrôle d'une partie non autorisée aux renseignements. La perte est involontaire de la part de l'institution et du bénéficiaire. Voici quelques exemples : • Livraison du courrier à la mauvaise adresse. • Élimination ou vente d'équipements ou d'appareils sans d'abord les purger de leurs renseignements personnels. • Perte de matériel ou de dossiers lors d'un déménagement ou par égarement	Cela correspond généralement au terme TI/sécurité : **atteinte à la disponibilité.** Cela pourrait également correspondre au terme TI/sécurité **atteinte à la confidentialité** en cas d'accès inapproprié ou non autorisé aux informations perdues.
Le **vol** se produit lorsqu'une partie non autorisée prend intentionnellement le contrôle de renseignements personnels de sorte que l'institution n'y a plus accès.	Cela correspond généralement à une **atteinte à la confidentialité**. Cela pourrait également correspondre à une **atteinte à l'intégrité** lorsque les informations sont inutilisables ou à une **atteinte**

Voici quelques exemples : • Vol d'équipement ou d'appareil insuffisamment chiffrés • Retrait des dossiers papier de l'institution	**à la disponibilité** lorsque les informations sont inaccessibles
Un **accès inapproprié et non autorisé** se produit lorsqu'une partie non autorisée (sans « besoin de connaître»), par ses propres actions, accède à des renseignements personnels. Leurs actions peuvent être intentionnelles ou non. Voici quelques exemples : • Un employé fouineur ou tout autre abus des privilèges d'accès. • Des cyberattaques, par exemple, un rançongiciel, un logiciel malveillant.	Cela correspond généralement au terme TI/sécurité : **Atteinte à la confidentialité**, qui inclut l'accès inapproprié ou non autorisé d'informations. Cela pourrait également correspondre à une **atteinte à l'intégrité** où les informations sont modifiées.
Autres infractions aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, y compris la collecte, l'usage, la création, la conservation non autorisées ou inappropriées de renseignements personnels. Voici quelques exemples : • Collecter ou créer des renseignements personnels qui ne sont pas directement liés à un programme ou une activité. • Utiliser des renseignements personnels à des fins non autorisées. • Supprimer ou éliminer accidentellement ou prématurément de renseignements personnels. • Ne pas éliminer les renseignements personnels conformément aux calendriers d'élimination établis.	Les autres atteintes doivent être considérées individuellement en fonction de leur lien avec la terminologie de la TI et de sécurité.

Cause de l'atteinte : Ces informations sont importantes pour décider des mesures à prendre pour éviter une répétition de l'atteinte à la vie privée. Ce formulaire regroupe les causes des atteintes en trois catégories :

- **Cause externe – Cyberincident :** Toute tentative non autorisée d'accéder, de modifier, de détruire, de supprimer ou de rendre indisponible un réseau de la TI ou une ressource du système.

  Conseil : Pour obtenir de plus amples renseignements sur les cyberincidents, veuillez consulter les groupes appropriés dans votre institution, de même que le Glossaire du Centre canadien pour la cybersécurité et l'Avis de mise en œuvre de la protection des renseignements personnels 2022-01 : Incidents de cybersécurité mettant en cause des renseignements personnels du SCT.

- **Cause externe – Général :** inclut l'ingénierie sociale et le vol.

  Conseil : Pour obtenir de plus amples renseignements sur l'ingénierie sociale, veuillez

consulter la page Tromperie et manipulation : les techniques de piratage psychologique du Commissariat.

- **Cause interne :** Fait référence aux actions des employés de l'institution, ainsi que des tiers agissant dans le cadre d'une entente, d'un accord ou d'un contrat avec l'institution. La liste des causes couvre à la fois les actions intentionnelles et non intentionnelles.

  Conseil : obtenir de plus amples renseignements sur les causes de cette catégorie, veuillez consulter les ressources suivantes sur le site Web du Commissariat :

  - Conseils clés en matière de protection des renseignements personnels à l'intention des professionnels des ressources humaines du gouvernement fédéral
  - Dix trucs pour empêcher les employés de fureter
  - Conseils à l'intention des institutions fédérales sur l'utilisation des dispositifs de stockage portatifs

B.4. Description : Fournir autant de détails que possible sous chaque question, sans inclure de renseignements personnels. Si des renseignements supplémentaires sont requis, le Commissariat ou le SCT communiquera avec l'institution. Pour les questions qui ne s'appliquent pas à l'atteinte, indiquer « sans objet » sur le formulaire.

Remarques concernant les questions 2, 3, 6 et 8 :

2. Cette question vise à déterminer les tiers impliqués dans l'atteinte, tels que des entrepreneurs ou d'autres institutions fédérales, et à établir leur rôle dans l'atteinte. Cette question n'a pas pour but de déterminer les personnes touchées par l'atteinte, les parties qui ont obtenu un accès non autorisé ou des destinataires non autorisés ou des renseignements personnels.
3. Fournir des renseignements détaillés sur l'emplacement géographique de l'atteinte (région au Canada, à l'étranger, etc.) et sur l'emplacement physique où l'atteinte s'est produite (p. ex., salle du courrier, vol dans un véhicule). Par exemple, si l'atteinte a été causée par une perte de courrier, indiquer l'origine, la destination prévue et toute information connue sur l'endroit où le courrier a été perdu.

6. Cette question consiste à établir l'initiative institutionnelle dans le cadre de laquelle l'atteinte s'est produite (p. ex., un programme d'avantages sociaux). Cette question n'est pas destinée à déterminer les applications ou les systèmes de la TI.

8. Cette question vise à déterminer toute relation entre les parties qui ont eu un accès non autorisé aux renseignements personnels, les destinataires probables des renseignements personnels et une ou plusieurs des personnes touchées. La relation peut être professionnelle ou personnelle. Ces informations sont importantes pour déterminer le risque réel de préjudice grave pour un individu et comment atténuer ce préjudice.

B.5. Mesures de sécurité : Cette question vise à établir les mesures de sécurité qui étaient en place lorsque l'atteinte s'est produite. Ces informations sont importantes pour décider des mesures à prendre pour éviter une répétition de l'atteinte à la vie privée. Pour faciliter son utilisation, ce formulaire fait référence aux types de mesures de sécurité mentionnés dans la *Directive sur les pratiques relatives à la protection de la vie privée* et la *Politique sur la sécurité du gouvernement*.

Type de mesure de sécurité	Exemples
Mesures de protection administratives	Politique de sécurité institutionnelle; dispositions de sécurité dans un contrat de service pour la destruction de documents.

Type de mesure de sécurité	Exemples
Mesures de protection physiques	Salles de stockage verrouillées, classeurs verrouillés.
Mesures de protection techniques	Chiffrement; dispositifs de contrôle d'accès électroniques, contrôles de vérification.

Conseil : Pour obtenir de plus amples renseignements sur les types de mesures, veuillez consulter :

- Annexe A de la *Directive sur les pratiques relatives à la protection de la vie privée*
- La *Directive sur la gestion de la sécurité*, comprenant :
  - Annexe B : Procédures obligatoires relatives aux mesures de sécurité de la technologie de l'information
  - Annexe C : Procédures obligatoires relatives aux mesures de sécurité matérielle
  - Annexe E : Procédures obligatoires relatives aux mesures de sécurité de la gestion de l'information

B.6. Sur qui portaient les renseignements personnels? En plus de préciser si l'atteinte a touché des clients, des bénéficiaires de services ou des employés fédéraux, vous êtes encouragés à utiliser l'option « autre » pour signaler des informations pertinentes supplémentaires sur les personnes touchées, dans la mesure où elles sont connues. Par exemple, les personnes touchées font-elles partie d'un groupe qui peut être particulièrement susceptible d'être blessé ou préjudiciable en raison de l'atteinte, comme un mineur, une victime d'un crime ou une personne en situation économique vulnérable? Ces informations sont importantes, car elles guident l'évaluation du risque réel de préjudice pour un individu.

La catégorie « autre » pourrait également inclure les répondants à l'enquête, les participants aux groupes de travail ou les commentateurs des médias sociaux.

Quels catégories et types de renseignements personnels l'atteinte a-t-elle compromis, dans la mesure où cela est connu? Passer en revue les catégories pour déterminer l'étendue des informations compromises par l'atteinte. Ensuite, indiquer tous les types d'informations compromises par l'atteinte. Par exemple, les types d'informations sur la santé peuvent inclure des antécédents médicaux ou un dossier médical (p. ex., une ordonnance ou un résultat de test). Les « coordonnées » peuvent inclure le nom, le numéro de téléphone, le numéro de téléphone portable, l'adresse électronique, l'adresse civique, le code postal, la ville de résidence et les adresses précédentes. Les « informations démographiques » peuvent inclure les données sur l'ascendance ou les renseignements relatifs à son éducation, à sa race, à son origine nationale ou ethnique, à sa couleur, à son âge ou à sa situation de famille.

L'inclusion de ces informations permettra de garantir que le formulaire est rempli.

Fiches de renseignements personnels et numéro d'enregistrement au SCT : Si les renseignements personnels faisant l'objet de l'atteinte ont été collectés à des fins administratives, indiquer le FRP concerné en fournissant le titre du FRP, le numéro du FRP et le numéro d'enregistrement au SCT. Si les FRP pertinents ne sont pas connus au moment du rapport initial, fournir une mise à jour dès que possible. Il arrive parfois que les renseignements personnels faisant l'objet de l'atteinte n'aient pas été destinés à être utilisés à des fins administratives. Par exemple, les renseignements recueillis accidentellement à partir d'une correspondance non sollicitée ne font pas partie d'un processus décisionnel. Dans ces cas-là, les informations ne seraient pas saisies dans un FRP, donc aucun numéro de FRP ne peut être cité. S'il n'y a pas de FRP applicable ou si le FRP pertinent est inconnu au moment du rapport initial, indiquer « sans objet » ou « inconnu » lorsque le titre et le numéro du FRP sont demandés.

B.7. Risques réels anticipés de préjudice grave pour un individu : Une atteinte substantielle à la vie privée est une atteinte dont on peut raisonnablement s'attendre à ce qu'elle crée un risque réel de préjudice grave pour une personne. Pour faciliter son utilisation, ce formulaire répertorie les types de préjudices graves

énoncés dans la *Politique sur la protection de la vie privée* et propose des exemples de moyens susceptibles de permettre ces préjudices. Les types de préjudices et les exemples de moyens fournis ci-dessous sont illustratifs et non exhaustifs.

Types de préjudices graves	**Exemples de moyens susceptibles de causer des préjudices**
Lésions corporelles	Chantage; vol d'identité; localiser physiquement et/ou communiquer avec une personne de telle sorte que cela permette de commettre une infraction criminelle (p. ex., impliquant des menaces ou des dommages physiques).
Dommage à la réputation et aux relations	Honte publique.
Perte financière/effets négatifs sur le dossier de crédit/perte d'emploi ou de possibilités commerciales ou professionnelles	Chantage; fraude sur les comptes bancaires; exploitation financière; vol d'identité; fraude par carte de paiement; humiliation publique.
Vol d'identité	Hameçonnage.
Dommages ou perte de biens	Perte de dossiers; hameçonnage; localiser physiquement et/ou communiquer avec une personne de telle sorte que cela permette de commettre une infraction criminelle (p. ex., impliquant des menaces ou des dommages physiques).

Conseil : Pour obtenir de plus amples renseignements sur l'évaluation du risque de préjudice pour une personne, veuillez consulter la Trousse d'outils de gestion des atteintes à la vie privée du SCT.

C.1. Avis aux personnes touchées : La *Directive sur les pratiques relatives à la protection de la vie privée* impose aux institutions d'inclure la notification des personnes touchées par une atteinte à la vie privée dans les mesures d'atténuation qu'elles doivent adopter en réponse à une atteinte substantielle de la vie privée, à moins que la notification ne soit inappropriée pour des raisons de sécurité, de confidentialité, juridiques ou autres.

- Les **avis directs** peuvent être envoyés par téléphone, courriel, lettre ou en personne.
- Les **avis indirects** font référence aux avis effectués par des informations publiées sur le site Web de l'institution ou des comptes de réseaux sociaux, des avis publiés ou dans les médias.

La méthode choisie dépend des circonstances et doit être déterminée par l'institution au cas par cas. L'avis indirect ne devrait généralement être utilisé que lorsque les individus ne peuvent pas être localisés ou lorsqu'il y a tellement de personnes qu'un avis direct serait inopportun ou trop coûteux.

C.2. Avis à d'autres organisations : Si une atteinte touche des renseignements personnels détenus par l'institution, mais qui ne sont pas sous son contrôle, la *Directive sur les pratiques relatives à la protection de la vie privée* exige que l'institution avise sans délai l'institution qui contrôle les renseignements personnels. Si plusieurs organisations sont énumérées, numérotez-les et utilisez ce numéro de référence pour indiquer la date à laquelle elles ont été notifiées dans le champ ci-dessous. Pour obtenir de plus amples renseignements sur l'avis à d'autres organisations, veuillez consulter l'annexe I : Norme sur le signalement des incidents de sécurité de la *Directive sur la gestion de la sécurité*.

D. Limitation et atténuation de l'atteinte : La question B.2 concerne la limitation immédiate de l'atteinte (c'est-à-dire l'arrêt de l'atteinte). La section D concerne les mesures ultérieures et continues de limitation et d'atténuation des atteintes prises par l'institution, y compris le contact avec des destinataires non autorisés,

lorsque cela est approprié et sûr, pour tenter de récupérer tout document ou copie de document compromis par l'atteinte.

En plus d'énumérer les mesures de confinement, inclure toutes les mesures prises ou prévues pour atténuer le risque réel de préjudice grave pour un individu. En voici quelques exemples :

- Réinitialiser le mot de passe.
- Offrir des services de surveillance du crédit, le cas échéant.
- Récupérer des informations mal acheminées.
- Demander à des destinataires inattendus de confirmer qu'ils ont détruit et non diffusé les informations.
- Informer les tiers qui peuvent réduire le risque de préjudice, tel que les processeurs de paiement, les institutions qui ont délivré des documents compromis et les institutions qui peuvent utiliser les informations compromises pour des décisions administratives.

Cette information est particulièrement importante lorsque le Commissariat détermine où il doit offrir des conseils ou recommander des solutions. Mettre à jour ces informations dans un rapport modifié s'il y a des changements entre les actions planifiées et les mesures finales de confinement et d'atténuation des atteintes prises par votre institution.

E. Prévention des atteintes à la vie privée

Conseil : Pour obtenir de plus amples renseignements sur la prévention et la réponse à une atteinte à la vie privée, veuillez consulter :

- Trousse d'outils de gestion des atteintes à la vie privée du SCT
- Prévenir une atteinte à la vie privée et réagir en cas d'atteinte sur le site Web du Commissariat