



Code de bonnes pratiques du numéro d'assurance sociale

17 mars 2026



Code de bonnes pratiques du numéro d'assurance sociale

Les formats en gros caractères, braille, MP3 (audio), texte électronique, et DAISY sont disponibles sur demande en [commandant en ligne](#) ou en composant le 1 800 O-Canada (1-800-622-6232). Si vous utilisez un téléscripteur (ATS), composez le 1-800-926-9105.

© Sa Majesté le Roi du chef du Canada, 2026

Pour des renseignements sur les droits de reproduction :
droitdauteur.copyright@HRSDC-RHDCC.gc.ca.

PDF

N° de cat. SG5-106/2025F-PDF

ISBN 978-0-660-77391-9



Table des matières

Liste des abréviations.....	0
1. Introduction.....	1
1.1 Contexte	2
2. Renseignements pour les titulaires de NAS	3
2.1 Obligations principales des titulaires de NAS	5
2.2 Renseignements sur le NAS pour les étudiants	7
2.3 Renseignements sur le NAS pour les nouveaux arrivants et les résidents temporaires.....	8
2.4 Engagement de Service Canada envers les titulaires de NAS	9
2.5 Les choses à faire et à ne pas faire : quand fournir votre NAS.....	10
3. Renseignements pour les employeurs	12
3.1 Obligations principales des employeurs	12
3.2 Information sur l'utilisation du NAS et les employeurs	15
3.3 Engagement de Service Canada envers les employeurs	15
3.4 Liste des choses à faire et à ne pas faire à l'intention des employeurs : demande, collecte, utilisation et archivage du NAS	16
4. Renseignements à l'intention des organisations du secteur privé.....	18
4.1 Principales obligations des organisations du secteur privé	18
4.2 Renseignements sur l'utilisation du NAS dans le secteur privé	20
4.3 Engagement de Service Canada envers les organisations du secteur privé	21
4.4 Liste des choses à faire et à ne pas faire à l'intention du secteur privé : demande, collecte, utilisation et archivage du NAS.....	22
5. Renseignements à l'intention du gouvernement et des partenaires de Service Canada.....	24
5.1 Obligations principales de Service Canada et des autres ministères et organismes autorisés.....	25
5.2 Communication des renseignements sur le NAS, Service Canada et autres ministères et organismes autorisés.....	28
5.3 Engagement de Service Canada envers les autres ministères et organismes autorisés	28



5.4 Utilisations fédérales autorisées du NAS	29
6.Obligations des employés de Service Canada	30
6.1 Exactitude, protection des renseignements personnels et sécurité – obligations principales des employés et des entrepreneurs de Service Canada.....	30
6.2 Les renseignements sur le NAS et les employés de Service Canada.....	32
6.3 Engagement de Service Canada envers ses employés.....	33
7.Sécurité du NAS : pratiques exemplaires contre les violations et la fraude.....	35
7.1 Savoir reconnaître les arnaques.....	36
7.2 Liste des choses à faire et à ne pas faire à l'intention des titulaires de NAS : protéger votre NAS ..	37
7.3 Que faire si vous soupçonnez que votre NAS a été compromis	39
7.4 Que faire si votre organisation traite des atteintes à la vie privée liées aux NAS.....	40





Liste des abréviations

AE

Assurance-emploi

ARC

Agence du revenu du Canada

CAEC

Commission de l'assurance-emploi du Canada

CPRP

Chef de la protection des renseignements personnels

CPVP

Commissariat à la protection de la vie privée du Canada

DGSI

Direction générale des services d'intégrité

EDSC

Emploi et Développement social Canada

IRCC

Immigration, Réfugiés et Citoyenneté Canada

LMEDS

Loi sur le ministère de l'Emploi et du Développement social

LPRPDE

Loi sur la protection des renseignements personnels et les documents électroniques

MDSC

Mon dossier Service Canada

NAS

Numéro d'assurance sociale

RAS

Registre d'assurance sociale

RPC

Régime de pensions du Canada



RQAP

Régime québécois d'assurance parentale

RRQ

Régime des rentes du Québec

SCT

Secrétariat du Conseil du Trésor



1. Introduction

Dans cette section

- [Aperçu](#)
- [1.1 Contexte](#)

Aperçu

Le Code de bonnes pratiques du NAS énonce les rôles et les obligations des utilisateurs du NAS. Les utilisateurs comprennent :

- les particuliers;
- les employeurs;
- le secteur privé et les organismes à but non lucratif;
- Service Canada et ses partenaires fédéraux et provinciaux;
- les employés de Service Canada.

Le Code de bonnes pratiques a pour but :

- d'établir un ensemble de règles claires pour protéger les renseignements personnels, assurer la sécurité des informations et l'exactitude des données lors de l'utilisation et de la gestion des numéros d'assurance sociale (NAS);
- de mieux faire connaître l'obligation commune de protéger le NAS contre l'utilisation inappropriée et la fraude;
- de fournir des normes afin d'aider tous les utilisateurs du NAS à comprendre leurs obligations et à s'en acquitter.

Le Code de bonnes pratiques respecte et explique les lois, politiques et directives pertinentes. En voici quelques exemples :

- [Loi sur le ministère de l'Emploi et du Développement social](#) (LMEDS);
- [Loi sur l'assurance-emploi](#);
- [Loi sur la protection des renseignements personnels](#);
- [Loi sur la protection des renseignements personnels et les documents électroniques](#) (LPRPDE);
- [Politique sur la protection de la vie privée](#);
- [Directive sur le numéro d'assurance sociale](#).

Ces documents précisent l'utilisation du NAS. Plus de 150 lois provinciales et territoriales font référence au NAS. Pour connaître des exigences particulières, consultez votre gouvernement

provincial ou territorial. Les utilisateurs du NAS doivent respecter ces lois et politiques fédérales et provinciales.

1.1 Contexte

Le NAS est un numéro unique à 9 chiffres. La *Loi sur le ministère de l'Emploi et du Développement social* (LMEDS) le définit comme un numéro de dossier ou de compte ou pour le traitement des données. Le programme du NAS a été lancé en 1964 avec un objectif simple : permettre l'inscription des personnes à l'assurance-emploi.

Au fil du temps, il a commencé à être utilisé à d'autres fins. En 1965, le [Régime de pensions du Canada](#) (RPC) et le [Régime de rentes du Québec](#) (RRQ) ont adopté le NAS comme numéro de dossier. En 1967, le NAS est également devenu un numéro de dossier aux fins de l'impôt sur le revenu.

Aujourd'hui, le NAS est utilisé pour gérer les dossiers d'emploi, les déclarations fiscales et l'accès aux programmes gouvernementaux. Un NAS est désormais requis pour la majorité des personnes qui travaillent au Canada, ainsi que pour celles qui demandent des prestations et des services gouvernementaux. À Service Canada, nous délivrons un NAS à vie à chaque personne. Personne ne peut s'approprier le NAS d'une autre personne. Il est très important de protéger l'intégrité du NAS pour aider à protéger les personnes, les organisations et le gouvernement contre la fraude et l'utilisation abusive.

Le NAS n'est pas une pièce d'identité. Il s'agit d'un numéro confidentiel utilisé exclusivement à des fins administratives. Pour éviter les vols et empêcher l'utilisation du NAS comme pièce d'identité, le gouvernement a cessé de produire des cartes de NAS physiques en 2014. Désormais, les personnes reçoivent une lettre de confirmation en personne ou par courrier, ou une lettre de confirmation numérique par l'entremise de MDSC pour confirmer leur NAS.

2. Renseignements pour les titulaires de NAS

Dans cette section

- [Aperçu](#)
- [2.1 Obligations principales des titulaires de NAS](#)
- [2.2 Renseignements sur le NAS pour les étudiants](#)
- [2.3 Renseignements sur le NAS pour les nouveaux arrivants et les résidents temporaires](#)
- [2.4 Engagement de Service Canada envers les titulaires de NAS](#)
- [2.5 Les choses à faire et à ne pas faire : quand fournir votre NAS](#)

Aperçu

La [Loi sur le ministère de l'Emploi et du Développement social](#) (LMEDS) et la [Loi sur l'assurance-emploi](#) précisent qui a besoin d'un NAS pour travailler. La liste inclut :

- les citoyens canadiens;
- les résidents permanents;
- les résidents temporaires.

Un NAS est également nécessaire pour recevoir des prestations et des services des programmes gouvernementaux.

Le [Règlement sur l'assurance-emploi](#) exige que vous ayez un NAS à des fins d'emploi. Vous devez fournir votre NAS à votre employeur au plus tard trois jours après la date de début de votre emploi. Si vous n'avez pas déjà un NAS, cela ne vous empêche pas de travailler. Toutefois, vous devez présenter votre demande de NAS dans les trois jours suivant votre date de début d'emploi. Vous devez ensuite fournir votre NAS à votre employeur au plus tard 3 jours après la date à laquelle vous l'avez reçu.

En vertu de la [Loi de l'impôt sur le revenu](#), vous avez besoin d'un NAS :

- pour remplir votre déclaration de revenus;
- pour faire une [demande d'assurance-emploi](#) (AE);
- pour [vous inscrire au Régime de pensions du Canada](#) et au [Régime de rentes du Québec](#) (RPC/RRQ).

Certaines entités du secteur privé doivent vous demander votre NAS. Elles le font pour tous les comptes et placements qui rapportent des revenus (comme des intérêts et des dividendes). Cela comprend :

- les banques;

- les coopératives de crédit;
- les sociétés de fiducie.

Si vous gagnez des revenus en tant que vendeur sur une plateforme numérique, vous êtes désormais tenu de communiquer votre NAS aux exploitants de la plateforme numérique à des fins fiscales. Les vendeurs dont les renseignements seront recueillis et communiqués à l'ARC peuvent inclure ceux qui participent à ces activités :

- la vente de marchandises;
- la location de biens immeubles ou réels (résidentiels et commerciaux);
- les services de covoiturage et de livraison;
- les services personnels.

Consultez [Les règles de déclaration pour les opérateurs de plateformes numériques](#) pour en savoir plus.

Le NAS est considéré comme un renseignement personnel en vertu de la [Loi sur la protection des renseignements personnels](#). Vous pouvez protéger votre vie privée en gardant le contrôle de vos renseignements personnels et en traitant votre NAS comme un renseignement confidentiel. À l'exception de certains programmes gouvernementaux, vous pouvez décider de la collecte et de l'utilisation de votre NAS. Vous ne devez le fournir que lorsque la loi l'exige. Vous pouvez ainsi éviter la fraude et préserver la confidentialité de vos renseignements personnels. Si vous le partagez autrement que dans les cas prévus par la loi, vous devez accepter le risque que cela comporte.

Il n'est pas interdit par la loi de demander le NAS d'une personne. De nombreuses organisations du secteur privé demandent votre NAS. Cela fait partie de leurs politiques et procédures. Mais à Service Canada, nous déconseillons de telles pratiques.

La [Loi sur la protection des renseignements personnels et les documents électroniques](#) (LPRPDE) est la loi fédérale sur la protection de la vie privée qui s'applique aux organisations du secteur privé. La LPRPDE protège votre droit à la vie privée.

La LPRPDE impose aux organisations du secteur privé de respecter certaines règles en matière de collecte, d'utilisation et de divulgation des données personnelles. Ces règles comprennent la mise en place de mesures de protection pour protéger vos données personnelles. Elles protègent vos données personnelles contre la perte, le vol ou la divulgation non autorisée.

Conformément à la LPRPDE, vous avez le droit :

- de savoir pourquoi une organisation recueille, utilise ou divulgue vos renseignements personnels;
- de vous attendre à ce qu'une organisation collecte, utilise ou divulgue vos renseignements personnels de manière appropriée;
- d'attendre d'une organisation qu'elle utilise les renseignements uniquement aux fins auxquelles vous avez consenti;

- de connaître les responsables de la protection de vos renseignements personnels au sein de l'organisation;
- d'attendre d'une organisation qu'elle protège vos renseignements personnels en prenant les mesures de sécurité appropriées;
- de vous attendre à ce que les renseignements personnels qu'une organisation détient à votre sujet soient exacts, complets et à jour;
- d'accéder à vos renseignements personnels et de demander des modifications;
- de porter plainte contre la manière dont une organisation traite vos renseignements personnels.

Pour en savoir davantage sur l'application de la LPRPDE à l'utilisation du NAS, consultez le site web du [Commissariat à la protection de la vie privée](#).

Rappel : La loi ne permet pas aux entreprises du secteur privé d'exiger le NAS des clients à des fins autres que la déclaration des revenus. Personne ne peut vous refuser un produit ou un service parce que vous avez refusé de fournir votre NAS lorsque la loi ne l'exige pas.

Pour vous renseigner davantage à ce sujet, veuillez consulter : [Protégez votre numéro d'assurance sociale](#).

2.1 Obligations principales des titulaires de NAS

En tant que titulaire du NAS, vous avez 4 obligations principales quand il s'agit de protéger votre NAS.

1. Ne donnez jamais votre NAS à moins d'être certain que la loi l'exige ou à moins d'être convaincu qu'il est nécessaire et que vous comprenez les risques.

Un aperçu des utilisations appropriées de votre NAS est présenté à la section [2.5, Les choses à faire et à ne pas faire : quand fournir votre NAS](#).

Vous devez fournir votre NAS pour participer à certains programmes et services gouvernementaux. Pour vous informer des lois fédérales et de l'utilisation des NAS par le gouvernement, consultez la [Directive sur le numéro d'assurance sociale](#) du Secrétariat du Conseil du Trésor du Canada.

Vous devez fournir votre NAS à votre employeur aux fins de l'impôt sur le revenu et des prestations. Dans certains cas, vous devez fournir votre NAS à certaines entités du secteur privé. Sauf lorsque la loi l'exige, c'est à vous de décider quand et à qui communiquer les renseignements relatifs à votre NAS.

Vous pouvez fournir votre NAS en dehors des utilisations prescrites par la loi. Toutefois, ce faisant, vous pourriez vous exposer à un risque accru de fraude ou de vol d'identité. Vous ne devriez le faire que si vous êtes disposé à assumer ce risque.

Certaines organisations du secteur privé vous demanderont votre NAS au moment de vérifier votre cote de crédit. Cela augmente la probabilité qu'ils vérifient ou mettent à jour les bons dossiers de crédit. Lorsqu'on vous demande votre NAS pour une vérification de crédit, vous n'êtes pas légalement tenu de

le fournir. Vous pouvez également fournir au demandeur une copie de votre rapport de solvabilité. Ce rapport de solvabilité ne devrait pas inclure votre NAS.

Personne ne peut vous refuser un produit ou un service parce que vous avez refusé de fournir votre NAS lorsque la loi ne l'exige pas. Si une organisation refuse de vous fournir un produit ou un service à moins de fournir votre NAS, vous pouvez porter plainte en suivant les instructions de la section ci-dessous (2.1.2).

2. Prenez des mesures pour protéger votre NAS contre le vol et l'utilisation abusive.

La [Loi sur la protection des renseignements personnels](#) définit le NAS comme un renseignement personnel. Par conséquent, tous les utilisateurs du NAS doivent s'efforcer de le protéger. Si une personne vole votre NAS, elle pourrait l'utiliser pour avoir accès à un vaste éventail de renseignements personnels, ainsi qu'à des prestations et services en votre nom. En tant que titulaire de NAS, vous avez des obligations importantes quand il s'agit de protéger votre NAS. Suivez la section [7.2, Liste des choses à faire et à ne pas faire à l'intention des titulaires de NAS : protéger votre NAS](#).

De nombreuses organisations ne sont pas au courant des utilisations appropriées du NAS. Agissez si vous croyez qu'une organisation privée ne protège pas convenablement vos renseignements personnels ou votre NAS. Parlez à la personne responsable si une organisation refuse de fournir le produit ou le service que vous avez demandé à moins que vous ne divulguiez votre NAS. Vous pouvez également utiliser le processus de plainte de l'organisation.

Si vous n'êtes pas satisfait de la réponse de l'organisation ou si vous soupçonnez qu'elle ne gère pas bien vos renseignements personnels :

- communiquez avec l'association sectorielle de l'organisation, son ombudsman ou son bureau des plaintes;
- déposez une plainte officielle contre l'organisation auprès du [Commissariat à la protection de la vie privée du Canada](#) en composant le 1-800-282-1376.

Par exemple, l'[Association canadienne du marketing](#) (en anglais seulement) et l'[Ombudsman des services bancaires et d'investissement](#) traitent les plaintes des clients au sujet de leurs sociétés membres.

3. Informez Service Canada et les autres autorités compétentes si vous avez une preuve qu'une organisation utilise votre NAS d'une manière frauduleuse

Les criminels peuvent utiliser un NAS volé ou perdu pour frauder des gouvernements, des organisations et des particuliers. Si quelqu'un d'autre utilise votre NAS pour travailler illégalement ou pour obtenir du crédit, les gouvernements peuvent vous imposer pour un revenu que vous n'avez pas gagné. Vous pourriez également éprouver des difficultés lorsque vous faites une demande de crédit. Même si vous prenez des mesures pour protéger vos renseignements personnels, vous pourriez quand même être victime d'un vol d'identité. Les voleurs sont de plus en plus créatifs lorsqu'ils tentent de voler des renseignements personnels. Si vous soupçonnez qu'une personne utilise votre NAS de façon frauduleuse, il est important d'agir rapidement. La section [7.3, Que faire si vous soupçonnez que votre NAS a été compromis](#) vous indique les mesures à prendre et les coordonnées pertinentes.

4. Communiquer avec Service Canada

Vous devriez communiquer avec Service Canada lorsque :

- vous modifiez légalement votre nom;
- votre statut de citoyen change;
- votre NAS temporaire expire;
- vous souhaitez mettre à jour votre désignation de genre;
- vous avez la preuve que quelqu'un utilise votre NAS d'une manière frauduleuse;
- vous découvrez que l'information contenue dans votre dossier de NAS est incorrecte ou incomplète.

Si vous avez oublié votre NAS, vous pouvez :

- le trouver sur votre déclaration de revenus, vos relevés fiscaux, votre relevé d'emploi ou vos cotisations à un Régime enregistré d'épargne-retraite (REER);
- le consulter et l'imprimer en vous connectant ou en vous inscrivant à [Mon dossier Service Canada \(MDSC\)](#);
- obtenir une confirmation de votre NAS en [présentant une demande](#).

Pour en savoir plus sur la manière de demander une confirmation de votre NAS, consultez le site Web sur la [Numéro d'assurance sociale](#).

Vous pouvez également communiquer avec Service Canada pour mettre à jour votre dossier du Registre d'assurance sociale (RAS).

- Si vous avez changé de nom, vous devez mettre à jour votre dossier de NAS. Et ce, quelle que soit la raison du changement de nom (mariage ou autre). Vous devez demander la mise à jour de votre dossier de NAS à votre nouveau nom dans les 60 jours suivant votre changement de nom.

Pour mettre à jour votre dossier de RAS, vous pouvez faire une demande :

- [en ligne](#);
- En personne, à un [Centre Service Canada](#);
- par la [poste](#).

2.2 Renseignements sur le NAS pour les étudiants

Éducation et NAS

- Vous n'avez pas à fournir votre NAS pour faire une demande dans un établissement d'éducation post-secondaire :
 - Université
 - Collège
 - Autres établissements d'enseignement
- Il se peut que vous deviez fournir votre NAS pour des raisons fiscales, par exemple :
 - se voir délivrer un Certificat pour frais de scolarité et d'inscription (T2202)
- Il se peut que vous deviez fournir votre NAS pour bénéficier de prestations et de services liés à l'éducation, par exemple :
 - Aide financière canadienne aux étudiants
 - Aide au remboursement
 - Programme canadien de prêts aux étudiants
 - Programme du prêt canadien aux apprentis

2.3 Renseignements sur le NAS pour les nouveaux arrivants et les résidents temporaires

L'emploi et votre NAS

- Vous avez besoin d'un NAS pour travailler au Canada
 - Si vous êtes résident temporaire au Canada, vous avez besoin d'un permis valide vous autorisant à travailler au Canada
 - Votre permis et votre NAS doivent avoir la même date d'expiration
- Vous pouvez travailler au Canada dès que vous avez demandé votre NAS
 - Si vous n'avez pas encore de NAS, vous pouvez quand même commencer à exercer un travail rémunéré si vous demandez votre NAS dans les trois jours après avoir commencé à travailler
 - Vous devez faire connaître votre NAS à votre employeur dans les 3 jours suivant votre entrée en poste ou dans les 3 jours suivant la réception de votre NAS
- Vous pouvez continuer à travailler au Canada si vous avez demandé le renouvellement de votre permis
 - Si vous avez demandé le renouvellement de votre permis de travail ou de votre permis d'études et que celui-ci expire avant qu'une décision ne soit prise à ce sujet, vous pouvez continuer à travailler (c'est ce qu'on appelle le « statut conservé »)
 - Si votre statut est conservé, vous pouvez continuer à travailler tandis que votre NAS est expiré
 - Ce n'est qu'une fois votre permis renouvelé et le permis officiel reçu que vous devez présenter une nouvelle demande au programme de NAS pour mettre à jour la date d'expiration de votre NAS

Se protéger et protéger son NAS

- Demander votre NAS gratuitement auprès du gouvernement du Canada
 - Il ne coûte rien de demander ou de renouveler un NAS
 - Vous ne devez autoriser personne à demander un NAS en votre nom, à moins qu'elle ne soit légalement autorisée à le faire
 - Il existe plusieurs façons de [demander votre NAS](#)
 - En ligne
 - En personne
 - Par la poste
 - Vous pouvez consulter votre NAS en toute sécurité dans votre [Mon dossier Service Canada](#) (MDSC)
- Attention aux arnaques et aux fraudes
 - Informez-vous et protégez-vous contre [les arnaques et les fraudes visant les nouveaux arrivants](#)
 - Si vous payez un représentant, comme un consultant en immigration ou un avocat, assurez-vous qu'il est titulaire d'un permis
 - [Vérifiez si votre représentant est autorisé](#) à représenter les immigrants ou à leur donner des conseils
- Protéger votre identité
 - Faites attention aux personnes à qui vous communiquez votre NAS, vos documents d'identité et vos renseignements personnels

2.4 Engagement de Service Canada envers les titulaires de NAS

À Service Canada, nous avons l'obligation de protéger le NAS d'une personne contre l'utilisation inappropriée, la fraude et le vol dans le contexte des prestations et des programmes du gouvernement fédéral. Nous prenons cette obligation très au sérieux et avons de nombreux moyens de protéger les NAS. Nous veillons également à l'exactitude des renseignements contenus dans le NAS. Cela comprend des pratiques bien définies et fonctionnelles qui servent à détecter et à contrer tout accès inapproprié aux renseignements personnels.

À Service Canada, nous :

- surveillons et limitons l'accès à votre NAS et à vos renseignements personnels;
- permettons l'accès uniquement aux personnes et aux organisations autorisées qui ont un « besoin de savoir »;
- vérifions soigneusement que l'identité des titulaires de NAS et des demandeurs est exacte pour assurer l'exactitude et la complétude des renseignements personnels;

- informons les titulaires de NAS sur la protection, l'utilisation et la divulgation appropriées du NAS;
- aidons tous les clients qui souhaitent obtenir des renseignements sur le NAS ou les services gouvernementaux connexes.

La [Section 5, Renseignements à l'intention de Service Canada et de ses partenaires](#), décrit les rôles et les obligations de Service Canada et de ses partenaires relativement au NAS.

2.5 Les choses à faire et à ne pas faire : quand fournir votre NAS

Vous ne devez fournir votre NAS que lorsque la loi l'exige. Si quelqu'un vous demande votre NAS, posez des questions. Il peut arriver que vous deviez fournir votre NAS parce que la loi l'exige. Dans d'autres cas, vous pouvez refuser de fournir votre NAS si la situation ne l'exige pas.

Il convient de fournir votre NAS lorsque :

- vous traitez avec le gouvernement pour certaines transactions
 - Vous devez fournir votre NAS pour :
 - déclarer vos impôts;
 - accéder à des programmes et prestations tels que l'assurance-emploi, les prêts et bourses d'études et les pensions publiques.
- vous êtes embauché(e) pour un emploi et commencez à travailler
 - Les employeurs doivent collecter votre NAS pour déclarer vos revenus au gouvernement, à des fins fiscales et de prestations sociales.
- vous ouvrez un compte qui génère des revenus (comme des intérêts et des dividendes)
 - Les institutions financières doivent collecter votre NAS pour déclarer vos revenus de compte et d'investissement au gouvernement à des fins fiscales.

Il ne convient pas de fournir votre NAS lorsque :

- vous traitez avec des entités non gouvernementales pour la plupart des transactions
 - Vous n'avez pas besoin de fournir votre NAS pour :
 - louer un bien, remplir une demande de location ou négocier un bail;
 - vous abonner à des services de télécommunication (tels que téléphone, Internet ou câble), à l'exception d'Hydro-Québec qui doit collecter le NAS en vertu de la législation provinciale;
 - louer une voiture;
 - remplir un questionnaire sur les antécédents médicaux;
 - rédiger un testament;
 - vous inscrire dans un établissement d'études postsecondaires.
- vous postulez à un emploi
 - Les employeurs n'ont pas besoin de votre NAS tant qu'ils ne vous ont pas embauché et que vous n'avez pas commencé à travailler et à percevoir des revenus.
- vous effectuez des opérations bancaires générales et des opérations financières qui ne génèrent pas de revenus

- vous n'avez pas à fournir votre NAS pour :
 - demander une carte de crédit;
 - demander ou renouveler un prêt hypothécaire;
 - demander un prêt ou une marge de crédit;
 - encaissez un chèque.
- vous demandez un rapport de solvabilité
 - Vous n'avez pas besoin de fournir votre NAS pour obtenir un rapport de solvabilité.
 - Proposez de fournir d'autres documents, au lieu de votre NAS, à des fins d'identification ou de crédit.

3. Renseignements pour les employeurs

Dans cette section

- [Aperçu](#)
- [3.1 Obligations principales des employeurs](#)
- [3.2 Information sur l'utilisation du NAS et les employeurs](#)
- [3.3 Engagement de Service Canada envers les employeurs](#)
- [3.4 Liste des choses à faire et à ne pas faire à l'intention des employeurs : demande, collecte, utilisation et archivage du NAS](#)

Aperçu

En tant qu'employeur, vous devez demander le numéro d'assurance sociale (NAS) de chaque employé que vous embauchez. Cela permet de fournir à chaque employé un relevé d'emploi (RE). Cela permet également de leur fournir divers relevés de fin d'exercice. Ces relevés comprennent, par exemple, le relevé T4 aux fins de l'impôt sur le revenu. Les employeurs utilisent aussi le NAS pour enregistrer et transmettre les retenues salariales des employés aux fins suivantes :

- [l'impôt sur le revenu](#);
- le programme de l'[assurance-emploi](#) (AE);
- le [Régime de pensions du Canada](#) (RPC) ou le [Régime des rentes du Québec](#) (RRQ);
- le [Régime québécois d'assurance parentale](#) (RAPQ).

3.1 Obligations principales des employeurs

En tant qu'employeur, vous jouez un rôle essentiel dans la protection du NAS contre l'utilisation abusive, la fraude et le vol. Vous devez vous assurer d'identifier correctement les employés et vous devez demander d'autres pièces d'identité avant de finaliser leurs documents d'emploi. La carte d'assurance sociale et la lettre de confirmation du NAS ne sont pas des documents d'identification ni des pièces d'identité. Les employés ne peuvent pas utiliser ces documents à cette fin.

Les employeurs du secteur privé peuvent également avoir des rôles et des obligations précis relativement au NAS et aux renseignements personnels. Renseignez-vous davantage sur les fonctions du secteur privé à la [Section 4, Renseignements à l'intention des organisations du secteur privé](#).

1. En vertu de la loi, vous devez demander le NAS de chaque nouvel employé au plus tard 3 jours après le début de l'emploi

Si un nouvel employé n'a pas de NAS et qu'il est autorisé à travailler au Canada, demandez-lui de [présenter une demande de NAS](#). Il doit le faire dans les trois premiers jours suivant le début de son emploi. Cela n'empêche pas l'employé de travailler avant d'obtenir son NAS. Il doit vous informer de son NAS dans les trois jours suivant la réception de sa lettre de confirmation du NAS.

Toute personne qui occupe un emploi assurable au Canada doit avoir un NAS. Ceci est conforme à la [Loi de l'impôt sur le revenu](#), au [Régime de pensions du Canada](#) et à la [Loi sur l'assurance-emploi](#).

Renseignez-vous sur la manière de confirmer le NAS d'un employé à la section [3.2, Information sur l'utilisation du NAS et les employeurs](#).

2. Vous devez vous assurer que les employés ayant un NAS commençant par le chiffre « 9 » sont autorisés à travailler au Canada

[Immigration, Réfugiés et Citoyenneté Canada](#) (IRCC) autorise les résidents temporaires à travailler au Canada. Ces résidents ne sont ni citoyens canadiens ni résidents permanents, et reçoivent des NAS qui commencent par le chiffre « 9 ».

Ces NAS sont valides en fonction des permis de travail d'IRCC. Ils correspondent à la date à laquelle le travailleur étranger peut travailler au Canada. Le NAS à lui seul ne leur permet pas de travailler. Vous devez vérifier toutes les modalités du permis de travail avant de les embaucher. Cela comprend les dates et les lieux de travail autorisés.

Si le document d'immigration d'un travailleur étranger expire, vous devez demander au travailleur d'obtenir un document valide avant de l'embaucher. Vous devez demander à l'employé de s'adresser à IRCC pour ce faire. Vous devez également informer le travailleur étranger qu'il doit présenter à Service Canada une demande accompagnée du nouveau document d'immigration. Cela servira à mettre à jour le dossier de NAS en y versant la nouvelle date d'expiration.

Un résident temporaire peut travailler en attendant la décision relative au renouvellement de son permis de travail ou d'études. Il peut travailler même si son permis expire avant que la décision soit reçue ou s'il attend son permis officiel par courrier. Dans de telles situations, les résidents temporaires peuvent continuer à travailler, étudier ou utiliser leur NAS aux mêmes conditions tant qu'ils demeurent au Canada. Cela est conforme à l'alinéa 186(u) et à l'article 189 du [Règlement sur l'immigration et la protection des réfugiés](#).

Ces conditions demeurent valides jusqu'à ce qu'IRCC décide si le permis de travail ou d'études sera renouvelé. Le résident temporaire a alors un « statut conservé » (précédemment connu sous le nom de statut implicite). Pour plus d'information, veuillez visiter la [page Web d'IRCC pour le statut conservé](#) ou notre site Web [Recevoir votre NAS et mettre votre dossier de NAS à jour](#). À titre d'employeur, vous devez vérifier le nouveau document d'immigration une fois que vous l'aurez obtenu. Vous devez vérifier que la décision d'IRCC permet à l'employé de continuer à travailler au Canada. Vous devez également vérifier la nouvelle date d'expiration. Vous devez informer l'employé qu'il doit mettre à jour son dossier de NAS en y versant la nouvelle date d'expiration.

Pour plus de renseignements, visitez le [site Web de l'IRCC](#). Vous pouvez également téléphoner au Centre d'appels d'IRCC au 1-888-242-2100 ou ATS : 1-888-576-8502.

3. Les employeurs doivent protéger les renseignements personnels de leurs employés, y compris les NAS, contre le vol et l'utilisation abusive

Les employeurs comme vous doivent conserver et éliminer les renseignements personnels des employés de manière sûre et sécuritaire. Seules les personnes autorisées peuvent accéder à ces renseignements. Vous devez tenir des registres des cotisations au RPC, des cotisations à l'AE et des impôts que vous retenez ou déduisez. Vous devez conserver ces dossiers pendant au moins **6 ans** à compter de la fin de la dernière année où vous avez employé la personne concernée. Cela est conforme à la *Loi sur l'assurance-emploi*, au *Régime de pensions du Canada* et à la *Loi de l'impôt sur le revenu*.

La [Loi sur la protection des renseignements personnels et les documents électroniques](#) (LPRPDE) est la loi fédérale sur la protection des renseignements personnels pour les organisations du secteur privé. Cela inclut les employeurs du secteur privé. La LPRPDE exige que les organisations privées se conforment aux politiques lorsqu'elles recueillent, utilisent ou divulguent des données personnelles dans le cadre de leurs activités commerciales. Les données personnelles peuvent comprendre le NAS.

Ces politiques incluent la mise en place de mesures de sécurité. Vous devez suivre la section [3.4, Les choses à faire et à ne pas faire à l'intention des employeurs : demande, collecte, utilisation et archivage du NAS](#).

Si quelqu'un vole, utilise ou divulgue le NAS d'un employé de façon frauduleuse, vous devez agir rapidement. Voir la section [7.4, Que faire si votre organisation traite des atteintes à la vie privée liées aux NAS](#).

4. Les employeurs doivent informer Service Canada s'ils soupçonnent qu'un NAS est mal utilisé

Vous jouez un rôle de premier plan dans la détection et la prévention de la fraude liée aux NAS. L'emploi illégal et l'évasion fiscale sont deux des principaux motifs de fraude liée au NAS. Chaque année, des criminels et d'autres acteurs utilisent des cartes d'assurance sociale ou des lettres de confirmation volées, perdues, empruntées ou fausses. Les fraudeurs s'en servent pour escroquer des individus, des organisations du secteur privé et des gouvernements.

Si vous soupçonnez qu'un NAS a été compromis ou est utilisé à des fins frauduleuses, vous devez immédiatement signaler le problème. Vous devez fournir à Service Canada votre numéro d'entreprise délivré par l'ARC. Vous devez également fournir des renseignements pour authentifier l'entreprise et le titulaire du NAS. Pour ce faire, vous pouvez consulter notre site Web [Communiquer avec le programme du numéro d'assurance sociale](#).

3.2 Information sur l'utilisation du NAS et les employeurs

Vos employés n'ont pas besoin de vous présenter une preuve matérielle de leur NAS. Ils n'ont pas besoin de vous fournir leur carte d'assurance sociale ou une lettre de confirmation.

Seuls les employeurs peuvent vérifier le NAS d'un employé auprès du programme de numéro d'assurance sociale. Les fournisseurs de services de paie ne peuvent pas communiquer avec nous pour vérifier un NAS, car ils ne sont pas l'employeur. Néanmoins, les fournisseurs de services de paie doivent recevoir les NAS des employés. Cela leur permet de s'acquitter de leurs rôles et responsabilités envers leur client ou l'employeur.

Il devrait y avoir une entente contractuelle entre le fournisseur de services de paie et l'employeur pour expliquer ce besoin. Ces organisations doivent se conformer au présent [Code de bonnes pratiques du NAS](#).

Pour confirmer le NAS d'un employé actuel ou ancien, communiquez avec notre [programme de numéro d'assurance sociale](#). Vous devez fournir votre numéro d'entreprise délivré par l'[Agence du revenu du Canada](#) (ARC). Vous devez également fournir des renseignements pour authentifier l'entreprise et le titulaire du NAS. Cela peut comprendre :

- son nom;
- sa date de naissance.

De nombreuses personnes utilisent un surnom, un second prénom ou un autre nom. Vous devez vous assurer d'identifier correctement vos employés. Vous devez inscrire le nom légal de votre employé. Vous pouvez rappeler aux employés que leur dossier de NAS doit refléter leur nom légal actuel.

Vous **ne** devez **pas** utiliser le NAS comme identificateur d'employé. De graves problèmes pourraient survenir si les renseignements personnels des employés sont à risque. Nous vous invitons vivement à utiliser une autre méthode d'identification des employés. Cette mesure vise à protéger la vie privée de vos employés et à maintenir l'intégrité du NAS.

3.3 Engagement de Service Canada envers les employeurs

La fraude d'identité, y compris les NAS volés, perdus et empruntés, peut entraîner des coûts accrus. Ces coûts peuvent causer des préjudices aux particuliers, aux organisations du secteur privé et aux gouvernements. La protection du NAS est essentielle à la gestion et à la prestation de nombreux services gouvernementaux et programmes de prestations. Vous pouvez aider à prévenir la fraude et l'utilisation abusive du NAS.

Empêchez les personnes non autorisées d'accéder aux dossiers des employés qui contiennent le NAS. Vous pouvez également signaler une utilisation abusive soupçonnée du NAS. Chacun doit faire sa part pour s'assurer que ses renseignements personnels sont exacts et complets. Service Canada prend cette obligation très au sérieux. Nous avons de nombreuses façons de protéger les NAS et l'exactitude des renseignements personnels.

Pour nous acquitter de cette obligation envers les employeurs, nous nous engageons à :

- confirmer ou fournir le NAS de leurs employés;
- offrir des conseils, de l'information et des outils pour aider les employeurs à s'acquitter de leurs obligations relatives au NAS;
- aider les employeurs lorsque l'information du NAS dont ils ont la garde est menacée;
- collaborer avec les employeurs pour détecter, signaler et enquêter sur les cas soupçonnés d'utilisation abusive d'un NAS.

Pour obtenir une description complète des rôles et obligations de Service Canada liés au NAS, consultez la section [5.1, Obligations principales de Service Canada et des autres ministères et organismes autorisés](#).

3.4 Liste des choses à faire et à ne pas faire à l'intention des employeurs : demande, collecte, utilisation et archivage du NAS

À faire

- Demander le numéro d'assurance sociale (NAS) de tout nouvel employé, si la loi l'exige, dans les 3 jours suivant le début de son emploi

Cela n'empêche pas la personne de travailler avant d'obtenir son NAS. Elle peut continuer à occuper un emploi assurable.

- Enregistrer le NAS de l'employé dans une zone sécurisée ou sur un système informatique chiffré
- En cas de doute sur la validité du NAS d'un employé, communiquez avec le programme de numéro d'assurance sociale de Service Canada

Vous pourrez ainsi vérifier le numéro. Vous pouvez appeler le programme de numéro d'assurance sociale aux assurances sociales en composant le 1-866-274-6627 au Canada.

- Assurez-vous que la formation d'intégration de votre nouvel employé comprend les aspects importants de la confidentialité des renseignements personnels et du NAS
- Si le NAS d'un nouvel employé commence par « 9 », assurez-vous que le permis de travail est valide

Immigration, Réfugiés et Citoyenneté Canada (IRCC) délivre le permis de travail. Respectez toutes les modalités du permis de travail.

- Visitez le site Web [Pensez cybersécurité – Centre canadien pour la cybersécurité](#) pour connaître les pratiques exemplaires en matière de cybersécurité

Ces conseils vous aideront à assurer la sécurité des renseignements personnels et du NAS de vos employés.

À ne pas faire

- Ne demandez jamais le NAS sur une demande d'emploi ou pendant une entrevue.
- N'utilisez pas le NAS comme numéro d'identification d'employé; utilisez un identificateur unique à votre organisation.
- N'embauchez pas une personne qui n'a pas de NAS valide vérifié, sauf dans les cas où l'employé fournit la preuve qu'il a demandé un NAS.
- Ne donnez pas le NAS d'un employé à qui que ce soit à moins que cette personne soit autorisée par la loi à obtenir ce renseignement (par exemple, aux fins de l'impôt sur le revenu ou des prestations gouvernementales).
- N'embauchez jamais une personne sans vous être préalablement assuré qu'elle est autorisée à travailler dans votre industrie au Canada.
- Ne permettez pas que les fraudes relatives au NAS demeurent non signalées; signalez l'utilisation frauduleuse soupçonnée d'un NAS en communiquant avec Service Canada.
- Ne laissez pas de documents contenant les renseignements personnels ou les NAS des employés à la vue de tous.

4. Renseignements à l'intention des organisations du secteur privé

Dans cette section

- [Aperçu](#)
- [4.1 Principales obligations des organisations du secteur privé](#)
- [4.2 Renseignements sur l'utilisation du NAS dans le secteur privé](#)
- [4.3 Engagement de Service Canada envers les organisations du secteur privé](#)
- [4.4 Liste des choses à faire et à ne pas faire à l'intention du secteur privé : demande, collecte, utilisation et archivage du NAS](#)

Aperçu

Les organisations du secteur privé peuvent recueillir le numéro d'assurance sociale (NAS) à des fins légalement autorisées, notamment pour l'emploi, la déclaration de revenus et les programmes de prestations gouvernementales.

Certaines organisations utilisent également le NAS pour d'autres raisons, comme la vérification de la cote de crédit et l'identification. Service Canada déconseille d'utiliser le NAS à ces fins. Dans ce [Rapport du vérificateur général sur le NAS](#), on laisse entendre que ces pratiques mettent en danger l'intégrité du NAS. Elles font augmenter le risque de fraude et d'abus liés au NAS.

Le [Commissariat à la protection de la vie privée du Canada](#) recommande aux organismes de s'abstenir de demander le NAS de leurs clients lorsque la loi ne l'exige pas. Les clients ont le droit de refuser de fournir leur NAS à moins que la loi ne l'exige.

Rappel : Les organismes du secteur privé ne sont légalement tenus de demander un NAS que pour la déclaration des revenus. Vous ne pouvez pas refuser un produit ou un service à un client qui refuse de fournir son NAS lorsque la loi ne l'exige pas.

4.1 Principales obligations des organisations du secteur privé

La [Loi sur la protection des renseignements personnels et les documents électroniques](#) (LPRPDE) est la loi fédérale sur la protection des renseignements personnels pour les organisations du secteur privé. Cela inclut les employeurs du secteur privé. La loi concilie le droit à la vie privée d'une personne et le besoin d'une organisation de recueillir, d'utiliser ou de communiquer des renseignements personnels. Les NAS sont considérés comme étant des renseignements personnels au sens de la LPRPDE.

La LPRPDE exige que les organisations du secteur privé se conforment aux règles régissant la collecte, l'utilisation et la divulgation des renseignements personnels (y compris les NAS) dans le cadre de leurs activités commerciales. Ces règles comprennent la mise en place de mesures de sécurité

visant à protéger les données personnelles contre la perte, le vol ou la divulgation non autorisée.

[Innovation, Sciences et Développement économique Canada](#) assure la gestion globale des politiques de la LPRPDE.

Une organisation du secteur privé a 4 obligations clés en ce qui concerne la protection du NAS, ce qui respecte les principes de la LPRPDE.

1. Une organisation du secteur privé ne doit jamais utiliser le NAS comme pièce d'identité ou comme numéro d'identification du client

Le NAS n'est ni un document d'identification ni une pièce d'identité. Par conséquent, personne ne devrait considérer le NAS comme une identification officielle du gouvernement. Pour vérifier l'identité d'un client, demandez plutôt une pièce d'identité appropriée qui comprend des éléments de données précis. Cela peut comprendre :

- un nom;
- une date de naissance;
- un lieu de résidence.

Vous ne devriez jamais demander le NAS d'un client à moins qu'il ne soit légalement nécessaire de le recueillir. La loi n'oblige pas les entreprises du secteur privé à exiger le NAS des clients à des fins autres que la déclaration des revenus. Si votre organisation du secteur privé recueille le NAS d'un client, vous devez vous conformer à la LPRPDE ou aux lois provinciales applicables. Cela comprend la divulgation des fins d'utilisation du NAS et l'obtention du consentement. Vous devez utiliser le NAS uniquement aux fins exposées.

Si votre organisation privée doit attribuer un numéro d'identification à ses clients, vous devez en créer un.

2. Si vous demandez le NAS d'un client, vous devez lui dire pourquoi vous le demandez et vous ne devez l'utiliser qu'à cette fin

Il n'y a qu'une raison pour laquelle une organisation du secteur privé a légalement besoin du NAS des clients. Les banques, les coopératives de crédit et les sociétés de fiducie ont besoin du NAS pour les comptes et les placements qui rapportent des revenus (comme les intérêts et les dividendes). Par exemple, les institutions financières ont besoin du NAS pour déclarer les intérêts versés dans le compte bancaire d'une personne. Si un compte ne produit pas de revenu, la loi n'exige pas que votre organisation demande le NAS du client.

Les opérateurs de plateformes numériques sont désormais tenus de recueillir un numéro d'identification fiscale (NIF), comme le NAS, auprès des utilisateurs qui génèrent des revenus sur leurs plateformes. Cette mesure est prise aux fins de l'impôt sur le revenu. Consultez [les règles de déclaration pour les opérateurs de plateformes numériques](#) pour en savoir plus.

Lorsque vous demandez le NAS d'un client pour une raison autre que la déclaration de revenus, la loi n'oblige pas le client à fournir son NAS. Vous devez informer votre client que dans ces cas, fournir son NAS est facultatif et doit être consensuel.

3. Une organisation du secteur privé ne peut pas demander aux clients de fournir leur NAS sans que la loi l'exige

Vous devriez en informer vos clients. Vous devez obtenir le consentement d'un client pour recueillir et utiliser son NAS. Si la loi n'exige pas de fournir un NAS, vous devriez offrir au client un moyen de retirer son consentement. Cette option devrait être disponible en tout temps après que le client vous a fourni son NAS. Le mécanisme pour retirer son consentement doit être clair, facile à appliquer, sûr et efficace.

4. Les organisations du secteur privé doivent protéger les renseignements personnels de leurs clients (y compris les NAS) du vol et d'une utilisation ou divulgation frauduleuse

Si vous recevez les renseignements personnels de vos clients, vous devez les protéger. Vous devez vous assurer que les renseignements sont protégés contre le vol, l'utilisation inappropriée ou la divulgation. Votre organisation devrait garder les NAS sous clé lorsqu'ils sont conservés sur papier. Vous devriez chiffrer ou protéger par mot de passe les NAS en format numérique. Vous devriez également conserver les NAS à l'écart des autres renseignements personnels.

Les organisations du secteur privé sont encouragées à suivre les indications de la section [4.4, Liste des choses à faire et à ne pas faire à l'intention du secteur privé : demande, collecte, utilisation et archivage du NAS](#).

Si quelqu'un vole le NAS de vos clients ou l'utilise de façon inappropriée, vous devez agir. Si votre organisation est assujettie à la LPRPDE, une déclaration obligatoire peut être exigée. Si la violation de l'information personnelle présente un risque réel de préjudice important pour un individu, le signalement est obligatoire. Il peut également y avoir des exigences de rapport équivalentes au niveau provincial. Pour plus d'informations, voir la section [7.4, Que faire si votre organisation traite des atteintes à la vie privée liées aux NAS](#).

4.2 Renseignements sur l'utilisation du NAS dans le secteur privé

Service Canada déconseille fortement aux organisations privées de demander le NAS comme pièce d'identité pour les raisons suivantes :

- le NAS ne comporte aucune caractéristique de sécurité permettant d'identifier la personne;
- le secteur privé est incapable de vérifier les renseignements contenus dans le NAS;
- il y a un risque accru pour les entités du secteur privé qui utilisent uniquement le NAS à des fins d'identification;
- cette pratique augmente aussi les risques que des usurpateurs d'identité ciblent l'organisme.

Si votre organisation souhaite toujours demander un NAS uniquement à des fins d'identification, vous ne devez en aucun cas laisser entendre qu'il s'agit d'une obligation. Vous ne pouvez pas exiger le NAS pour établir une relation d'affaires. Vous devez clairement indiquer qu'il est optionnel de fournir le NAS, et offrir au client d'autres options.

Avant de donner leur NAS, les clients ont le droit de demander les exigences légales dans lesquelles s'inscrit la collecte du NAS. De plus amples renseignements sur le NAS sont disponibles sur la page [Aperçu du NAS](#).

La loi n'exige pas de fournir une preuve matérielle du NAS (carte ou lettre de confirmation). Les organisations du secteur privé n'ont pas à demander une preuve du NAS d'un client.

Vous devriez adopter une politique d'ouverture avec vos clients. Les clients ont le droit de savoir quelles informations vous détenez à leur sujet. Vous devriez communiquer volontiers les dossiers personnels au client auquel ils appartiennent. Pour en savoir plus sur le principe de transparence de la LPRPDE, visitez le site Web du [Commissariat à la protection de la vie privée](#).

Avant la création de la LPRPDE, les organisations du secteur privé n'étaient pas tenues d'obtenir le consentement des clients pour la collecte des NAS. Les dispositions de la LPRPDE s'appliquent à tous les renseignements personnels détenus par une organisation, peu importe à quel moment ceux-ci ont été recueillis. Dans certains cas, la destruction ou l'effacement de dossiers plus anciens peut être le meilleur moyen de traiter cette information. Néanmoins, il n'est pas toujours nécessaire pour les organisations comme la vôtre de demander le consentement pour continuer à détenir et à utiliser les NAS au dossier.

Pour décider si vous devez conserver le NAS d'un client, posez la question suivante : Est-il nécessaire de conserver les renseignements en raison d'une loi ou d'un contrat? Si la réponse est « oui », considérez les questions suivantes.

- Les renseignements sont-ils (ou ont-ils déjà été) utiles ou nécessaires?
- Est-il probable que le client s'attende à ce que l'organisation conserve le NAS dans ses dossiers?

Si la réponse à ces questions est « non », il est préférable d'éliminer ces NAS de façon sécuritaire.

4.3 Engagement de Service Canada envers les organisations du secteur privé

Service Canada s'engage à offrir des conseils, des renseignements, de la formation et des outils aux organisations. Cette mesure vise à aider les organisations comme la vôtre à s'acquitter de leurs obligations de protection du NAS.

Pour obtenir une description complète des rôles et obligations de Service Canada liés au NAS, consultez la section [5.1, Obligations principales de Service Canada et des autres ministères et organismes autorisés](#).

4.4 Liste des choses à faire et à ne pas faire à l'intention du secteur privé : demande, collecte, utilisation et archivage du NAS

À faire

- Identifiez correctement le client en demandant des preuves d'identité valides (le NAS n'est pas une pièce d'identité).
- Obtenez le consentement de votre client avant de recueillir, d'utiliser ou de communiquer des renseignements personnels le concernant, y compris son numéro d'assurance sociale (NAS).
- Offrez aux clients une solution de rechange au NAS lorsqu'une vérification de crédit est nécessaire.
- Informez les clients du type de renseignements personnels que vous recueillez, de la raison pour laquelle ils sont recueillis et des fins auxquelles votre entreprise les utilisera.
- Conservez les renseignements de nature délicate dans un endroit protégé ou dans un système informatique chiffré limité au « besoin de savoir ».
- Déchiquez tous les documents papier dont vous n'avez plus besoin et effacez ou retirez les documents électroniques contenant des renseignements personnels comme le NAS avant leur élimination.
- Choisissez une personne au sein de votre organisation ou entreprise qui agira à titre de chef de la protection des renseignements personnels (CPRP).

Le CPRP traite toutes les questions de confidentialité. Établissez un cadre de gestion de la protection des renseignements personnels qui comprend des pratiques vérifiables en matière de respect de la vie privée et de sécurité. Veillez à ce que le CPRP relève de la haute direction. Le CPRP doit avoir le pouvoir d'intervenir sur les questions de protection des renseignements personnels dans votre organisation. Prenez au sérieux la sécurité des données et la protection des renseignements personnels.

- Formez tous les employés sur les politiques de confidentialité.

Tenez-les informés. Ainsi, ils pourront répondre aux questions et aux préoccupations continues des clients. Faites en sorte que ces politiques soient accessibles à tous les employés.

À ne pas faire

- N'utilisez pas les renseignements personnels des clients, y compris le NAS, à des fins qui vous sont interdites.
- N'utilisez pas le NAS comme numéro d'identification du client ou pour identifier quelqu'un dans le cadre de transactions commerciales régulières.
- Ne recueillez pas le NAS et d'autres renseignements personnels, sauf si la loi l'exige.
- Ne demandez pas les renseignements personnels d'un client, et surtout le NAS, par courriel.

- Ne mettez aucun renseignement personnel du client sur Internet.
- Ne vendez pas ou ne fournissez pas les renseignements personnels des clients à des organisations ou entreprises tierces à moins d'avoir obtenu le consentement de vos clients.
- Ne divulguez pas le NAS d'une personne à qui que ce soit, à moins de savoir que cette personne a le droit d'obtenir ces renseignements en vertu de la loi.
- Ne refusez pas à un client un produit ou un service parce qu'il a refusé de fournir son NAS, à moins que la loi exige qu'il fournisse ce renseignement (par exemple, pour un produit de revenu enregistré).

5. Renseignements à l'intention du gouvernement et des partenaires de Service Canada

Dans cette section

- [Aperçu](#)
- [5.1 Obligations principales de Service Canada et des autres ministères et organismes autorisés](#)
- [5.2 Communication des renseignements sur le NAS, Service Canada et autres ministères et organismes autorisés](#)
- [5.3 Engagement de Service Canada envers les autres ministères et organismes autorisés](#)
- [5.4 Utilisations fédérales autorisées du NAS](#)

Aperçu

La [Commission de l'assurance-emploi du Canada](#) (CAEC) a le pouvoir d'attribuer des numéros d'assurance sociale (NAS). La [Loi sur le ministère de l'Emploi et du Développement social](#) (LMEDS) et le [Règlement sur le numéro d'assurance sociale](#) confèrent ces droits à la CAEC. La CAEC a également le pouvoir de tenir à jour le Registre d'assurance sociale (RAS).

La CAEC a confié la responsabilité d'émettre et d'administrer les NAS à la Direction générale des services d'intégrité (DGSI). La DGSI se trouve au sein du ministère de l'Emploi et du Développement social du Canada (EDSC)/Service Canada.

À Service Canada, nous sommes responsables :

- d'élaborer des politiques et directives opérationnelles sur le NAS;
- d'administrer l'immatriculation des demandeurs de NAS et de tenir à jour le RAS;
- de traiter les demandes d'accès à l'information sur le NAS;
- d'élaborer et de mettre en œuvre des mesures d'enquête et de contrôle pour détecter et prévenir les utilisations abusives du NAS;
- d'élaborer des stratégies de communication avec les entreprises et le grand public;
- de réviser les lois relatives au NAS.

Le Secrétariat du Conseil du Trésor (SCT) et Service Canada, au nom de la Commission, sont tous deux responsables de la politique sur l'utilisation du NAS. Le SCT gère la [Directive sur le numéro d'assurance sociale](#), qui guide les ministères et organismes gouvernementaux sur la collecte et l'utilisation du NAS. Nous gérons le Code de bonnes pratiques du NAS.

Nous collaborons avec un large éventail d'organisations pour exécuter le programme du NAS. Service Canada et ses partenaires, comme vous, s'engagent à utiliser correctement le NAS. Nous veillons également à ce que des mesures soient en place pour protéger les renseignements personnels des personnes dans le cadre de l'exécution des programmes.

Les partenaires du NAS de Service Canada sont des organismes fédéraux et provinciaux qui acceptent officiellement de communiquer les renseignements contenus dans le Registre ou d'y accéder.

5.1 Obligations principales de Service Canada et des autres ministères et organismes autorisés

Seuls les ministères et organismes autorisés peuvent obtenir des renseignements provenant du RAS. Voici les mesures qui éclairent cet échange de renseignements du RAS :

- la LMEDS;
- La [Directive sur le numéro d'assurance sociale](#) du SCT;
- une entente d'échange de renseignements officielle.

À Service Canada, nous nous engageons à protéger les renseignements personnels des clients. Il en va de même pour les autres ministères et organismes autorisés. Nous devons également nous assurer que les renseignements contenus dans le RAS sont exacts, complets et sécurisés. Pour ce faire, nous et d'autres ministères et organismes autorisés avons les obligations principales suivantes.

1. Service Canada et les autres ministères et organismes autorisés doivent restreindre l'accès aux renseignements du RAS et leur communication

Des ententes officielles régissent l'accès du programme aux renseignements contenus dans le RAS, notamment en ce qui concerne les éléments suivants :

- les renseignements qui peuvent être consultés ou divulgués;
- les fins auxquelles les renseignements peuvent être consultés et par qui;
- les politiques et les procédures.

Sans entente, les entités ne peuvent pas accéder aux renseignements contenus dans le RAS. Conformément aux pratiques exemplaires en matière de protection des renseignements, nous limitons l'accès au RAS au plus petit nombre d'éléments de données nécessaires pour accomplir le travail. Nous surveillons la conformité aux modalités de l'entente, lesquelles peuvent faire l'objet d'une vérification. Service Canada et ses partenaires doivent utiliser une méthode sécurisée pour communiquer tout renseignement. Service Canada précise la méthode sécurisée à utiliser.

2. Service Canada et les autres ministères et organismes autorisés doivent s'efforcer de protéger les renseignements personnels contre le vol, l'accès inapproprié ou la divulgation

Service Canada et ses partenaires doivent respecter toutes les lois et politiques du gouvernement du Canada en matière de protection des renseignements personnels et de sécurité. Cela comprend la [Loi sur la protection des renseignements personnels](#) et la [Politique sur les services et le numérique](#) du Secrétariat du Conseil du Trésor. Service Canada et ses partenaires doivent également respecter toutes les politiques, procédures et pratiques en matière de protection des renseignements personnels et de sécurité relatives aux NAS. Service Canada et ses partenaires doivent informer les employés de toutes les politiques et procédures.

Service Canada et ses partenaires doivent également s'assurer que les employés ont suivi toute la formation requise et ont fait l'objet d'une enquête de sécurité appropriée. Nous surveillons qui accède aux dossiers de NAS au moyen de registres d'accès. Nous le faisons pour détecter tout accès inapproprié ou suspect. Nous pourrions ensuite examiner et traiter les cas défavorables.

Des mesures correctives sont en place pour les cas de non-conformité. Celles-ci peuvent mener à des mesures punitives. En cas d'atteinte substantielle à la vie privée, vous devez en informer les intervenants concernés. Il s'agit du Commissariat à la protection de la vie privée du Canada et du Secrétariat du Conseil du Trésor du Canada.

3. Service Canada et les autres ministères et organismes autorisés doivent confirmer l'identité des clients

Il est important de les identifier avec exactitude. Cela permet de s'assurer que le bon client reçoit la bonne prestation ou le bon service. C'est également essentiel pour prévenir l'utilisation frauduleuse. Service Canada et ses partenaires doivent confirmer l'identité d'un client. Ce faisant, nous devons respecter les ententes et les politiques de gestion de l'identité de Service Canada.

Ces politiques sont, entre autres :

- accepter uniquement les documents de preuve d'identité dont nous, à Service Canada, approuvons l'utilisation;
- examiner entièrement le dossier de NAS d'un client en comparant l'information provenant du RAS aux renseignements sur l'identité et le programme afin d'assurer la cohérence;
- corriger les renseignements qui figurent au dossier de NAS d'une personne si Service Canada ou ses partenaires y constatent une différence ou une erreur;
- agir si le document contient une annotation ou une condition.

Dans un tel cas, les partenaires doivent consulter leur entente et les procédures connexes pour connaître les mesures à prendre. Cela peut inclure un renvoi aux Services nationaux d'enquête ou au [programme de numéro d'assurance sociale](#).

4. Service Canada est responsable des renseignements personnels conservés dans le RAS et les ministères et organismes autorisés contribuent à maintenir l'exactitude et l'exhaustivité de ces renseignements

Le fait que les renseignements contenus dans le RAS soient exacts et complets garantit que le bon client recevra la bonne prestation. Cela permet de protéger de la fraude tous les programmes qui utilisent le NAS. Service Canada et ses partenaires doivent respecter les politiques de gestion de l'identité de Service Canada.

Lorsqu'une personne avise un partenaire de Service Canada d'une erreur dans son dossier de NAS, ce partenaire doit communiquer avec Service Canada. S'il s'agit d'une erreur de saisie des données, nous vérifierons si nous pouvons :

- la corriger au téléphone;
- apporter la correction sans contacter le client.

Sinon, le programme de numéro d'assurance sociale collaborera avec vous, le partenaire, pour informer le client sur la façon de corriger les données. Le programme confirmera également les documents que le client devra fournir et les options de service qui sont à sa disposition. Cette approche est la même pour les cas où l'inexactitude n'est pas attribuable à une erreur de saisie des données.

5. Service Canada et les ministères et organismes autorisés doivent établir des pratiques de gestion et de surveillance des risques

Service Canada et des partenaires comme votre ministère ou organisme doivent cerner les secteurs à risque élevé. Cela vise à détecter et à prévenir la fraude et l'accès ou la communication non autorisés de renseignements provenant du RAS. Lorsque des renseignements personnels sont consultés, Service Canada et les partenaires doivent le documenter. Cela permet de faire le suivi de la conformité aux politiques et principes de respect de la vie privée, de sécurité et d'intégrité des programmes.

Service Canada et ses partenaires doivent suivre l'utilisation des renseignements personnels. Nous devons également détecter tout accès non autorisé ou toute modification des renseignements personnels. Si quelqu'un va à l'encontre de ces politiques et principes, nous devons le signaler aux fonctionnaires de Service Canada. Nous avons mis en place des fonctionnaires, des processus et des mécanismes qui agissent ensemble pour mener des enquêtes et limiter les incidents d'atteinte ou de fraude dans les programmes.

Pour vous informer des obligations individuelles des employés, consultez la [Section 6, Obligations des employés de Service Canada](#).

5.2 Communication de renseignements sur le NAS, Service Canada et autres ministères et organismes autorisés

La [LMEDS](#) régit la communication des renseignements provenant du RAS. En vertu du paragraphe 28.2(5) de cette loi, la CAEC ou son représentant peuvent autoriser la communication de renseignements du RAS aux partenaires comme vous.

Vous ne pouvez pas communiquer à une autre organisation des renseignements provenant du RAS que nous avons fournis à votre ministère ou organisme autorisé. C'est le cas même si cette organisation est un utilisateur autorisé. Les organisations qui souhaitent obtenir des renseignements du RAS doivent communiquer avec le programme du NAS.

Le programme du NAS vérifie que la partie requérante a la permission d'obtenir ces renseignements et que la demande respecte les modalités de l'entente officielle régissant l'accès aux renseignements contenus dans le RAS. Cela comprend le type de renseignements que les modalités de l'entente autorisent Service Canada à communiquer et la raison pour laquelle les renseignements sont requis.

Les employés des organisations autorisées qui demandent des renseignements sur le NAS, mais qui n'y ont pas accès, doivent communiquer avec le programme du NAS pour accéder à l'information. Le nom de l'employé doit également figurer sur la liste des employés du programme de numéro d'assurance sociale. Le programme confirmera des renseignements précis auprès de l'employé pour 2 raisons :

- s'assurer que la partie requérante est un employé autorisé;
- s'assurer que la raison de la demande est valide et respecte les modalités de l'entente.

Signalez les problèmes liés au respect du présent Code de bonnes pratiques ou d'autres politiques connexes. Pour les signaler, vous devez, en tant que partenaire, communiquer avec le fonctionnaire désigné dans votre entente.

5.3 Engagement de Service Canada envers les autres ministères et organismes autorisés

Compte tenu du rôle important que joue Service Canada auprès de ses partenaires, nous nous engageons à :

- collaborer avec tous les partenaires du RAS pour améliorer l'intégrité et l'exactitude des données du RAS;
- assurer le succès à long terme du RAS en créant et en maintenant :
 - une structure claire de gouvernance et d'application de la loi (définie dans les ententes et les modèles de financement)
 - une liste claire des besoins en matière de services
 - des protocoles clairs de communication de renseignements

- une communication ouverte et transparente;
- fournir des conseils, des renseignements et des outils pour aider les partenaires à assumer leurs obligations relatives au NAS.

5.4 Utilisations fédérales autorisées du NAS

Le Secrétariat du Conseil du Trésor (SCT) du Canada gère la [Directive sur le numéro d'assurance sociale](#). Cette directive régit la manière dont les institutions fédérales recueillent, utilisent et communiquent le NAS. Le SCT confère également à certains ministères et organismes fédéraux le pouvoir de recueillir, d'utiliser et de communiquer le NAS.

Les institutions fédérales ne peuvent recueillir ou utiliser le NAS qu'à des fins autorisées par la loi. Une institution du gouvernement fédéral doit disposer d'une autorité légale expresse ou implicite et de l'approbation du Conseil du Trésor.

Les utilisations autorisées du NAS décrites dans la [Directive sur le numéro d'assurance sociale](#) (annexe A) comprennent :

- la récupération de fichiers historiques;
- les enquêtes légales et la collecte et l'utilisation du NAS;
- d'autres fins liées à l'application des lois (y compris à des fins fiscales);
- certaines fins non administratives compatibles avec l'application de la [Loi sur la statistique](#), de la [Loi sur la Bibliothèque et les Archives du Canada](#) et de la [Loi sur le vérificateur général](#).

Pour en savoir plus sur les utilisations autorisées et pour obtenir la liste des programmes et des activités autorisés, consultez l'annexe A de la [Directive sur le numéro d'assurance sociale](#).

6. Obligations des employés de Service Canada

Dans cette section

- [Aperçu](#)
- [6.1 Exactitude, protection des renseignements personnels et sécurité – Obligations principales des employés et des entrepreneurs de Service Canada](#)
- [6.2 Les renseignements sur le NAS et les employés de Service Canada](#)
- [6.3 Engagement de Service Canada envers ses employés](#)

Aperçu

En tant qu'employé ou entrepreneur de Service Canada, vous jouez un rôle clé dans la protection de l'intégrité, de la confidentialité et de la sécurité des numéros d'assurance sociale (NAS). Le Registre d'assurance sociale (RAS) contient les NAS et les renseignements personnels des clients, qui sont conservés par Service Canada dans des dossiers de programme très sécurisés qui sont hautement confidentiels.

Vous devez respecter les procédures qui protègent la gestion des renseignements personnels. Il vous incombe d'identifier et d'authentifier les personnes de façon précise, et de traiter les renseignements personnels avec soin. Cela comprend **la collecte, la conservation, l'utilisation et la communication**. Le respect des procédures établies permet de prévenir la fraude et de garantir que les clients reçoivent les prestations ou les services appropriés.

6.1 Exactitude, protection des renseignements personnels et sécurité – Obligations principales des employés et des entrepreneurs de Service Canada

Il vous incombe d'identifier et de vérifier l'identité des personnes, ce qui permet de protéger les renseignements personnels des clients. Vous devez le faire correctement et de façon sécurisée. Vous jouez un rôle important dans la prévention de la fraude et le maintien de l'intégrité du Registre de l'assurance sociale (RAS) en veillant à ce que le bon client obtienne la bonne prestation ou le bon service aux fins prévues. Il vous incombe également de signaler les incidents de fraude réels et soupçonnés.

Remarque : Les entrepreneurs embauchés par Service Canada ou un partenaire qui ont accès à des renseignements comme les NAS ont les mêmes obligations que les employés de Service Canada. Les entrepreneurs doivent satisfaire à l'exigence relative au « besoin de savoir », détenir l'attestation de sécurité appropriée et suivre les pratiques décrites dans le Code de bonnes pratiques du NAS.

1. Tous les employés et entrepreneurs de Service Canada doivent protéger la confidentialité et la sécurité des renseignements personnels des clients

Vous avez l'obligation de protéger les renseignements personnels contre tout accès, utilisation ou communication non autorisés. Vous devez gérer votre accès aux réseaux électroniques de façon responsable. Vous devez signer une entente exécutoire à cet effet.

Vous devez respecter la législation et les politiques et lignes directrices gouvernementales. Le SCT et le [Code de valeurs et d'éthique du secteur public](#) les décrivent. Certaines politiques imposent d'autres restrictions aux renseignements très personnels contenus dans le RAS. Ces politiques confèrent certaines obligations de communication au programme de NAS. Vous devriez également respecter la [Directive sur les conflits d'intérêts](#) de la fonction publique.

Seuls les employés autorisés peuvent avoir accès aux renseignements contenus dans le RAS ou en demander l'accès. Pour ce faire, vous devez avoir un « besoin de savoir » précis lié aux obligations qui vous sont attribuées. Vous devez ensuite suivre les procédures établies. Pour accéder aux renseignements sur le NAS ou les communiquer, vous devez y être autorisé et vous devez être tenu de le faire en raison de vos obligations. Vous devez respecter les lois, politiques et procédures qui guident ces obligations.

Vous devez confirmer l'identité du demandeur avant de communiquer des renseignements sur le NAS. Cette étape permet de s'assurer que la personne qui reçoit les renseignements est le titulaire du NAS ou son représentant légal. Lorsque vous communiquez des renseignements sur le NAS à un autre employé de Service Canada, vous devez confirmer que cet autre employé est autorisé à y accéder.

Lorsque les partenaires autorisés envoient des demandes de renseignements sur le NAS, vous devez les acheminer au programme de NAS. Seuls les employés du programme peuvent communiquer des renseignements sur le NAS à ces partenaires.

2. Les employés de Service Canada doivent établir et vérifier l'identité d'une personne en appliquant toutes les politiques et procédures de Service Canada de façon précise et sécuritaire

Il est essentiel d'identifier les clients de façon précise et sécuritaire afin de réduire le risque de fraude. Cela permet également de s'assurer que le bon client obtient les bonnes prestations ou les bons services. Les employés, comme vous, qui immatriculent des demandeurs de NAS, doivent respecter toutes les politiques et procédures connexes. Ceux qui utilisent le NAS pour vérifier l'identité doivent comparer les renseignements d'identité fournis dans le Registre. Ce faisant, vous devez respecter les politiques de gestion de l'identité de Service Canada.

Vous devez examiner entièrement le dossier d'une personne dans le RAS pour confirmer que le NAS est valide. Vous devez également vous assurer qu'il n'y a pas d'annotations ou de conditions susceptibles d'en affecter l'utilisation. Vous devez respecter toutes les politiques, procédures et formations en ligne relatives au traitement des NAS.

3. Les employés de Service Canada doivent suivre un ensemble de règles pour s'assurer que l'information contenue dans le RAS est exacte et protégée contre les utilisations frauduleuses

Vous devez comparer minutieusement les renseignements contenus dans le RAS avec ceux fournis par le client. L'employé qui a relevé un problème doit corriger toute erreur, inexactitude ou divergence dans le dossier de NAS d'une personne. Au besoin, il faut appliquer les mécanismes et procédures internes. Vous devez consulter les lignes directrices pertinentes, les manuels de formation et les procédures concernant des directives particulières.

S'il s'agit d'une erreur de saisie des données, nous vérifierons si nous pouvons :

- la corriger au téléphone
- apporter la correction sans contacter le client

Sinon, le [programme de NAS](#) collaborera avec vous, le partenaire, pour informer le client sur la façon de corriger les données. Le programme confirmera également les documents que le client devra fournir et les options de service qui sont à sa disposition. Cette approche est la même pour les cas où l'inexactitude n'est pas attribuable à une erreur de saisie des données.

Il se peut que le dossier de NAS d'un client exige une attention particulière. Dans ce cas, vous devez agir de façon appropriée. Cela comprend le renvoi de la question aux enquêteurs des services d'intégrité. Les enquêteurs ou autres intervenants peuvent également diriger un employé vers le programme de NAS.

6.2 Les renseignements sur le NAS et les employés de Service Canada

Le dossier de NAS contient tous les renseignements personnels versés lors de la demande de NAS ou de la demande de modification des renseignements. La modification des renseignements pourrait inclure des changements de nom, par exemple. Le dossier du NAS contient des renseignements comme le nom d'une personne, sa date et son lieu de naissance, les noms de ses parents et, s'il y a lieu, sa date de décès.

Le cas échéant, le dossier peut comporter des conditions particulières liées au NAS. Le RAS indique également l'état des NAS inactifs et des NAS liés. Le dossier d'un NAS peut être en attente si la demande est en cours de traitement ou si un cas justifie une annotation dans le dossier de NAS.

Les employés de Service Canada qui ont accès au RAS ont leur propre code d'utilisateur unique. Avec ce code, le RAS consigne toutes vos actions (comme les transactions et les accès) effectuées sur le RAS. Le programme du NAS reçoit un rapport mensuel en vue du suivi de l'utilisation. Il peut demander une piste d'audit détaillée pour tout employé.

Il vous est interdit d'accéder à votre propre dossier de NAS ou de le mettre à jour. Il vous est également interdit d'accéder au dossier de NAS d'un membre de votre famille, d'un ami ou d'un collègue, ou de le mettre à jour. Vous ne pouvez accéder aux renseignements sur le NAS, les demander, les utiliser ou les communiquer que si cela fait partie des tâches qui vous sont confiées. Vous ne devez accorder à personne un traitement préférentiel. Cela inclut les membres de la famille, les amis et les collègues.

Cela signifie que vous ne devez pas prendre des mesures pour faire traiter leur demande en priorité par rapport aux autres. La direction prendra des mesures correctives si les employés enfreignent les règles d'une loi, d'un code ou d'une politique.

Les mesures punitives pour l'infraction aux règles comprennent la réprimande verbale et écrite, la suspension ou la rétrogradation. De telles mesures peuvent même comprendre le licenciement. La législation relative à Emploi et Développement social Canada comprend un [Code de protection des renseignements personnels](#). Il énonce des sanctions précises. Ces sanctions peuvent être imposées pour un accès non autorisé ou inapproprié, ou pour l'utilisation ou la communication de renseignements personnels. La sanction maximale est une amende de 10 000 \$ ou une peine d'emprisonnement de six mois.

Les employés autorisés de Service Canada qui n'ont pas directement accès au registre doivent communiquer avec le [programme de numéro d'assurance sociale](#) pour obtenir des renseignements sur le NAS. Le programme ne peut divulguer des renseignements que si votre groupe est un utilisateur autorisé du Registre et si votre nom figure sur la liste d'employés du programme. Des renseignements précis seront validés pour confirmer votre autorisation et la validité de votre demande.

6.3 Engagement de Service Canada envers ses employés

À Service Canada, nous nous engageons à donner à nos employés et à nos entrepreneurs les moyens de s'acquitter de leurs obligations. Nous nous engageons également à protéger le NAS d'une utilisation inappropriée, de la fraude et du vol. Les employés et les entrepreneurs doivent s'assurer que le registre est exact, complet et sécurisé. Nous nous engageons à :

- veiller à ce que vous connaissiez bien les procédures, les directives et les outils nécessaires pour :
 - vérifier l'identité
 - valider les documents de preuve d'identité
 - accéder au registre et le mettre à jour
 - détecter la fraude
- créer des outils de formation en ligne qui vous aident à comprendre et à remplir vos fonctions liées au Registre;
- vous fournir un système de soutien complet :
 - pour vous informer des principaux enjeux et priorités et pour répondre aux questions liées au NAS
 - incluant :
 - des coordonnateurs locaux et régionaux des NAS

- des centres d'appels spécialisés
- des outils intranet
- une communication régulière
- vérifier que vous comprenez vos obligations comme employé ou entrepreneur.

7. Sécurité du NAS : Pratiques exemplaires contre les violations et la fraude

Dans cette section

- [Aperçu](#)
- [7.1 Savoir reconnaître les arnaques](#)
- [7.2 Liste des choses à faire et à ne pas faire à l'intention des titulaires de NAS : protéger votre NAS](#)
- [7.3 Que faire si vous soupçonnez que votre NAS a été compromis](#)
- [7.4 Que faire si votre organisation traite des atteintes à la vie privée liées aux NAS](#)

Aperçu

Le Code de bonnes pratiques du NAS énonce l'obligation commune de maintenir la sécurité et l'intégrité du NAS. Il décrit également la façon de prévenir la fraude et de se protéger contre les atteintes potentielles à la protection des données.

À Service Canada, nous nous engageons à aider les victimes de fraude. Ce Code de bonnes pratiques est l'un des soutiens offerts par Service Canada aux victimes de fraude, en plus de contenir d'autres renseignements importants pour tous les utilisateurs du NAS.

La [LMEDS](#) interdit l'utilisation d'un NAS à des fins frauduleuses ou trompeuses. Elle interdit également la création, la reproduction ou la vente non autorisée d'un NAS.

Le programme du NAS ne délivre pas de nouveaux NAS de façon proactive. Selon le paragraphe 28.2(8) de la LMEDS, l'attribution d'un nouveau NAS se limite à des cas particuliers. Ces cas incluent ceux où il existe une preuve d'utilisation abusive du NAS (par exemple, pour obtenir du crédit ou des services) où la personne demande un nouveau NAS.

Le fait d'obtenir un nouveau NAS ne protégera pas une personne contre la fraude ou le vol. Le NAS précédent continuera d'exister et sera lié à cette personne dans le secteur privé. Pour mettre à jour ses dossiers, le propriétaire d'un nouveau NAS doit communiquer avec :

- ses institutions financières;
- ses créanciers;
- les fournisseurs de services de pension;
- les autres organismes gouvernementaux;
- ses employeurs (anciens et actuels).

Si un client obtient un nouveau NAS, il doit régulièrement faire le suivi de ses comptes et de ses rapports de solvabilité pour les deux NAS. Les programmes, les ministères et les organismes du gouvernement du Canada peuvent encore avoir l'ancien NAS du client au dossier. Il incombe au client de communiquer avec ces programmes, ministères et organismes pour mettre à jour son dossier. Ainsi, ces programmes, ministères et organismes pourront lier le nouveau NAS du client à leur(s) compte(s) de prestation(s).

7.1 Savoir reconnaître les arnaques

Méfiez-vous des appels téléphoniques, des textos des messages électroniques qui :

- prétendent que votre NAS est compromis;
- proposent de remplacer votre NAS;
- menacent de verrouiller ou d'annuler votre NAS;
- demander des paiements en retard, des cartes de crédit prépayées ou des cartes-cadeaux.

N'utilisez pas les renseignements de l'afficheur pour confirmer l'identité de l'appelant, car les criminels peuvent modifier l'information affichée et prétendre être :

- une autre personne;
- un représentant d'une entreprise;
- un représentant d'une entité gouvernementale.

[Informez-vous sur la prévention des arnaques et des fraudes](#) pour vous protéger et protéger votre NAS.

Service Canada nous ne vous appellera jamais et ne vous enverra jamais de courriel pour vous demander votre NAS ou votre numéro de carte de crédit. Une tactique courante des fraudeurs consiste à communiquer avec vous en se faisant passer pour des représentants du gouvernement du Canada (Service Canada) pour voler vos renseignements. Il peut arriver qu'une personne vous joigne par téléphone, par message texte, par la poste ou par courriel et prétende travailler pour le gouvernement du Canada (Service Canada). Cette personne pourrait demander votre NAS ou vos numéros de carte de crédit, de compte bancaire et de passeport. Elle pourrait même dire qu'elle a besoin de ces renseignements pour que vous puissiez recevoir un remboursement ou un paiement. Il s'agit de communications frauduleuses.

Une autre tactique courante de fraude consiste à aiguiller les personnes vers un site Web qui ressemble au site Web de Service Canada. Le site Web peut vous demander de vérifier votre identité en saisissant des renseignements personnels. Vous ne devriez pas répondre à ces communications.

Certains sites Web tiers peuvent prétendre vous aider à demander un NAS. Il se peut qu'ils essaient de vous faire payer des frais. Vous ne devriez jamais utiliser des sites Web tiers pour demander un NAS. Vos renseignements personnels pourraient ne pas être sécurisés et être utilisés à des fins

frauduleuses. [Demandez un NAS](#) de manière sécurisée et gratuite directement auprès de Service Canada. Vous pouvez présenter votre demande en ligne, en personne à un centre Service Canada ou par courrier.

Si vous recevez une communication qui semble provenir de Service Canada ou d'un de ses programmes, nous vous encourageons à vérifier notre site Web. Vous pouvez également communiquer avec notre [programme de numéro d'assurance sociale](#). Si vous avez répondu à ce qui peut ressembler à une communication trompeuse ou frauduleuse, veuillez communiquer avec le [Centre antifraude du Canada](#). Vous pouvez le faire par courriel à info@antifraudcentre.ca ou par téléphone au 1-888-495-8501. Vous pouvez également communiquer avec le [Bureau de la concurrence](#) pour obtenir de l'aide. Vous pouvez le joindre au moyen de son site Web ou en composant le 1-800-348-5358.

Pour en savoir plus, visitez le site Web [Communications non autorisées et trompeuses](#) de Service Canada.

7.2 Liste des choses à faire et à ne pas faire à l'intention des titulaires de NAS : protéger votre NAS

La meilleure façon de se protéger contre la fraude est de protéger ses renseignements personnels. Vous devez éviter de communiquer votre NAS, à moins que cela ne soit nécessaire. Si quelqu'un d'autre utilise votre NAS, signalez immédiatement la fraude. Pour en savoir plus, consultez le [site Web du NAS](#).

À faire

- **Conservez les renseignements relatifs à votre NAS en toute sécurité**
 - Conservez les documents sur lesquels figure votre NAS dans une armoire ou un coffre-fort verrouillé.
 - Cela comprend les lettres de confirmation du NAS, les cartes de NAS et les documents relatifs à l'impôt sur le revenu
 - Déchiquez les documents qui contiennent des renseignements personnels lorsque vous vous en débarrassez
 - Consultez votre NAS en toute sécurité dans votre [Mon dossier Service Canada \(MDSC\)](#)
- **Protégez votre courrier contre le vol**
 - Verrouillez votre boîte aux lettres, surtout si vous attendez une lettre de confirmation de votre numéro d'assurance sociale.
 - Retirez rapidement le courrier reçu dès sa livraison.
 - Demandez à Postes Canada de garder votre courrier si vous prévoyez vous absenter.

- **Communiquez votre NAS seulement lorsque vous savez que la loi l'exige**
 - Avant d'accepter de transmettre votre NAS, renseignez-vous sur l'objectif poursuivi et demandez si la loi l'exige. Assurez-vous que vous êtes convaincu qu'il est nécessaire de le fournir; ou
 - Proposez d'autres documents pour prouver votre identité (par exemple, votre passeport, votre carte d'assurance maladie ou votre permis de conduire).
 - La [Directive sur le numéro d'assurance sociale](#) dresse une liste des lois fédérales qui font référence au NAS.
- **Visitez le site Web [Pensez cybersécurité – Centre canadien pour la cybersécurité](#)** pour connaître les pratiques exemplaires en matière de cybersécurité afin d'assurer la sécurité de votre NAS.

À ne pas faire

- **N'utilisez pas votre carte ou lettre de NAS comme pièce d'identité**
 - Votre lettre ou carte de NAS n'est pas un document d'identité.
- **Ne transportez pas votre NAS sur vous en public et ne le laissez pas à la vue de tous.** Si vous perdez votre NAS ou si on vous le vole, quelqu'un pourrait l'utiliser frauduleusement.
 - Ne gardez pas votre carte ou lettre de NAS dans votre portefeuille ou sac.
 - Ne conservez pas de documents sur lesquels figure votre NAS dans un tiroir non verrouillé ou sur des appareils non protégés par un mot de passe.
 - Ne recyclez pas et ne vous débarrassez pas de documents sur lesquels figure votre NAS sans les déchiqueter.
- **Ne divulguez pas votre NAS à quiconque vous le demande**
 - Vous pouvez refuser de fournir votre NAS si la loi ne l'exige pas.
 - Si quelqu'un vous refuse un service ou un produit, vous pouvez déposer une plainte en matière de protection de la vie privée auprès du [Commissariat à la protection de la vie privée du Canada](#).
 - [Apprenez-en davantage](#) sur ce qu'il faut faire lorsque quelqu'un vous demande votre NAS.
- **Ne répondez pas à un courriel, un appel ou un message texte qui fait référence à votre NAS, à moins de savoir qu'il est légitime**
 - Ne communiquez jamais votre NAS par téléphone, à moins que vous n'ayez passé l'appel vous-même et que vous sachiez que la loi l'exige.

- **N'envoyez pas vos renseignements personnels ou votre NAS sur des appareils numériques, par exemple lorsque vous utilisez une connexion Internet non sécurisée.**
 - Faites attention :
 - aux messages de personnes que vous ne connaissez pas;
 - aux messages concernant quelque chose que vous n'attendiez pas ou que vous n'avez pas demandé;
 - aux offres, menaces et demandes;
 - aux demandes d'action urgente;
 - aux demandes de communication de renseignements personnels.
 - Soyez particulièrement prudent face aux messages qui prétendent provenir du gouvernement.
 - Si vous avez un doute, communiquez directement avec l'organisation et demandez si elle vous a contacté.

7.3 Que faire si vous soupçonnez que votre NAS a été compromis

Vous pourriez être victime de fraude ou d'usurpation d'identité si votre NAS est divulgué ou compromis. Vous devez détecter et signaler les fraudes potentielles le plus tôt possible. Cela aidera à vous protéger et à réduire les risques de préjudice. Si votre NAS est compromis ou volé, vous devez :

1. Essayez de savoir s'il s'agit d'un délit (par exemple vol ou fraude)

Dans l'affirmative, communiquez avec votre service de police local pour déposer une plainte. Demandez le numéro de dossier, le nom du policier et son numéro de téléphone. Assurez-vous que le rapport indique votre nom et votre NAS. Communiquez également avec le Centre antifraude du Canada au 1-888-495-8501. Ce centre d'appels national fournit des conseils et de l'aide pour contrer le vol d'identité.

2. Communiquez avec Equifax et TransUnion, les 2 agences nationales d'évaluation du crédit au Canada

Demandez un exemplaire gratuit de votre rapport de crédit afin de l'examiner et de repérer toute activité suspecte. Vous pouvez obtenir un rapport gratuit par année. Demandez à ce qu'un avertissement soit inclus dans votre dossier de crédit. Les créanciers seront ainsi tenus de communiquer avec vous avant d'ouvrir de nouveaux comptes à votre nom.

Coordonnées

- [Equifax](https://www.equifax.ca) : 1-800-465-7166
- [TransUnion](https://www.transunion.ca) : 1-800-663-9980

3. Informez votre banque et vos créanciers.

Cherchez les coordonnées au verso de vos cartes bancaires et de crédit.

4. Lorsque vous recevez du courrier, signalez toute irrégularité à Postes Canada (1-866-607-6301)

Cela peut comprendre, par exemple, des enveloppes ouvertes ou des états financiers ou documents manquants.

5. Vous pouvez toujours obtenir des conseils auprès de Service Canada

Apprenez-en davantage sur [la fraude et les violations de données](#), ainsi que sur la [protection de votre NAS](#).

7.4 Que faire si votre organisation traite des atteintes à la vie privée liées aux NAS

La présente section s'applique à toute organisation assujettie à la [LPRPDE](#) ou à toute autre loi provinciale ou territoriale. Respectez toutes les exigences ou lignes directrices fédérales, provinciales ou territoriales concernant le traitement des atteintes à la vie privée et des avis d'atteinte à la vie privée.

En l'absence de telles lignes directrices, les lignes directrices suivantes peuvent s'appliquer. Par exemple, ces lignes directrices peuvent s'appliquer en cas d'une atteinte à la protection des renseignements personnels d'employés non fédéraux. Les présentes lignes directrices expliquent les étapes à suivre pour aviser les autorités compétentes en cas de vol soupçonné ou de divulgation inappropriée de renseignements personnels tels que le NAS.

Étape 1 : Évaluez les dommages

Déterminez le type et la quantité de renseignements personnels dont la sécurité a été compromise. Découvrez quand cela s'est produit et quels renseignements ont été compromis. Si le cas concerne des fichiers numériques, vérifiez si les données étaient chiffrées. Voici d'autres questions à prendre en considération :

- Quels renseignements pourraient être menacés?
- Quand et comment l'incident s'est-il produit?
- Où et comment les renseignements ont-ils été stockés?
- Des mesures de sécurité étaient-elles en place?

Étape 2 : Communiquer avec les services de police et le Centre antifraude du Canada

Si un délit a été commis (par exemple vol, fraude), communiquez avec la police. Vous pourriez également vouloir communiquer avec le [Centre d'appel antifraude du Canada](#) (1-800-495-8501).

Étape 3 : Communiquer avec Service Canada

Service Canada peut vous aider à déterminer les prochaines étapes. Service Canada peut également vous aider à réduire les dommages causés aux victimes de la violation. Communiquez avec le [programme de numéro d'assurance sociale](#) de Service Canada.

Étape 4 : Communiquer avec les agences d'évaluation du crédit

Parlez à des spécialistes en fraude des deux agences nationales d'évaluation du crédit du Canada. Discutez du type d'avertissement que vous devez utiliser pour réagir à l'incident.

- [Equifax](#) : 1-800-465-7166
- [TransUnion](#) : 1-800-663-9980

Étape 5 : Communiquer avec le Commissariat à la protection de la vie privée du Canada

Si la violation comprend des renseignements personnels (y compris des NAS), vous devrez peut-être en aviser le [Commissariat à la protection de la vie privée du Canada \(CPVP\)](#). La loi l'exige si votre organisation est assujettie à la LPRPDE et si l'atteinte à la vie privée présente un risque réel de préjudice important pour une personne. Il peut également y avoir des exigences de rapport équivalentes au niveau provincial ou territorial. Pour de plus amples renseignements, veuillez consulter le site Web [Signaler une atteinte à la vie privée dans votre organisation](#).

Étape 6 : Communiquer avec toutes les personnes concernées

Si vous êtes tenu de faire rapport de la violation au Commissariat à la protection de la vie privée (CPVP) en vertu de la LPRPDE, vous devez également contacter les personnes concernées par écrit dès que possible. Si votre organisation relève des équivalents provinciaux de la LPRPDE, vous pouvez également être tenu d'informer les personnes concernées. La lettre doit :

- expliquer l'incident
- décrire les mesures prises
- expliquer le type de renseignement qui peut être menacé
- envisager de proposer des services gratuits de surveillance de la solvabilité
- donner des conseils sur ce que la personne touchée devrait faire
- donner de l'information et des ressources sur le NAS
- fournir les coordonnées aux fins de soutien ultérieur, notamment :
 - celles d'un représentant de l'organisation
 - celles des agences d'évaluation du crédit
 - celles de Service Canada