**(insérer le nom du conseiller/le nom de l’entreprise)**

**POLITIQUE**  DE CONFIDENTIALITÉ INTERNE **ET PROCÉDURES** **DE VIOLATION DE LA VIE PRIVÉE**

# Objectif

Pour s’assurer que :

1. Je suis en conformité avec les exigences réglementaires et d’autoréglementation en matière de confidentialité (« Règlements »).

b) La protection de la vie privée d’un client est traitée de manière professionnelle, dans un environnement sécurisé et surveillée de manière appropriée.

**Le responsable de la protection de la vie privée**

La personne responsable est **< nom>**

1. Moi, **< Nom du Conseiller>** suis le responsable de la protection de la vie privée et toutes les demandes / plaintes doivent m’être adressées
2. Moi, **< Nom du Conseiller>** suis désigné par les présentes comme responsable de l’application de cette politique

**Mon engagement**

Mes clients sont mon entreprise.  En tant que conseiller, on me confie certains des renseignements personnels les plus sensibles de mes clients.  Je dois respecter cette confiance et j’ai besoin que mes clients soient conscients de mon engagement à protéger les informations qu’ils fournissent dans le cadre de mes relations d’affaires avec moi.

Je recueille des renseignements personnels conformément aux lois applicables et aux pratiques commerciales éthiques, afin de fournir des services et de faire des affaires. Je limite les informations que je collecte à celles qui sont nécessaires ou liées à ces fins.

Je respecte les **dix principes de confidentialité**. Les principes sont fondés sur la loi du gouvernement fédéral sur la protection de la vie privée, la *Loi sur la protection des renseignements personnels et les documents électroniques.*

**1. Responsabilisation** : Une organisation est responsable des renseignements personnels sous son contrôle et désigne une ou plusieurs personnes qui sont responsables de la conformité de l’organisation aux principes suivants.

**2. Fins d’identification** : Les fins auxquelles les renseignements personnels sont recueillis doivent être déterminées par l’organisation au moment de leur collecte ou avant cette date.

**3. Consentement** : La connaissance et le consentement de la personne sont requis pour la collecte, l’utilisation ou la divulgation de renseignements personnels, sauf lorsqu’ils sont inappropriés.

**4. Limitation de la collecte** : La collecte de renseignements personnels est limitée à ce qui est nécessaire aux fins déterminées par l’organisation. Les informations doivent être collectées par des moyens équitables et légaux.

**5. Limitation de l’utilisation, de la divulgation et de la conservation** : Les renseignements personnels ne doivent pas être utilisés ou divulgués à des fins autres que celles pour lesquelles ils ont été recueillis, sauf avec le consentement de la personne ou tel que requis par la loi. Les renseignements personnels ne seront conservés que le temps nécessaire à la réalisation de ces objectifs.

**6. Exactitude** : Les renseignements personnels doivent être aussi exacts, complets et à jour que nécessaire aux fins pour lesquelles ils doivent être utilisés.

**7. Mesures de protection** : Les renseignements personnels sont protégés par des mesures de sécurité adaptées à la sensibilité de l’information.

**8. Transparence** : Une organisation doit mettre facilement à la disposition des individus des renseignements précis sur ses politiques et pratiques relatives à la gestion des renseignements personnels.

**9. Accès individuel** : Sur demande, une personne est informée de l’existence, de l’utilisation et de la divulgation de ses renseignements personnels et a accès à ces renseignements. Une personne doit pouvoir contester l’exactitude et l’exhaustivité de l’information et la faire modifier au besoin.

**10. Contestation de la conformité** : Une personne doit être en mesure de répondre à un défi concernant la conformité aux principes ci-dessus à la ou aux personnes désignées pour la conformité de l’organisation.

**Collecte et utilisation des informations**

Je recueille les renseignements nécessaires pour accomplir la tâche pour laquelle je suis engagé, qu’il s’agisse d’assurance, de produits financiers ou de plans financiers.

Les renseignements personnels sont des renseignements qui se réfèrent à vous en particulier. J’utiliserai des moyens justes et légaux pour recueillir vos renseignements personnels. Je ne recueillerai que des renseignements pertinents et conformes aux fins de la collecte. Dans la mesure du possible, je recueillerai les renseignements requis directement auprès du client, ou de son ou ses représentants autorisés, dans les demandes et les formulaires remplis, par d’autres moyens de correspondance, tels que le téléphone, le courrier ou Internet, et par le biais de leurs relations d’affaires avec moi.

**Ce que j’ai besoin de savoir et pourquoi**

Je recueille des renseignements auprès de mes clients et à leur sujet, uniquement avec leur consentement, ou tel que requis ou permis par la loi. En général, je recueillerai des renseignements personnels tels que leur nom, adresse, numéro(s) de téléphone ou autres informations d’identification, telles que leur numéro d’assurance sociale (NAS) ou leur date de naissance.

Le type d’informations supplémentaires que je recueille dépendra du type de produit ou de service concerné. Les renseignements recueillis peuvent être financiers, ce qui comprendrait des renseignements tels que le lieu de travail, le revenu annuel, l’actif et le passif. Il peut s’agir de placements ou de conseils, nécessitant des informations sur des éléments tels que vos objectifs financiers et vos plans de retraite. Si le client fait une demande d’assurance ou de prestations d’assurance collective, il peut également s’agir d’informations sur la santé ou le mode de vie, telles que sa profession, ses antécédents et ses plans de voyage, son dossier de conduite ou son casier judiciaire.

**Consentement**

Le consentement est pour moi d’établir un dossier et de recueillir et de maintenir des informations personnelles, médicales et financières et doit être signé par le client et placé dans son dossier.

**Protection des renseignements personnels**

En tant que conseiller, j’ai accès aux renseignements sur les clients et je dois comprendre la nécessité de garder les renseignements protégés et confidentiels. Mes procédures indiquent clairement que je dois utiliser l’information uniquement aux fins prévues.

Si j’embauche un membre du personnel, il devra signer un accord de confidentialité au début de son emploi.

**Conservation des renseignements personnels**

Je ne conserverai les renseignements personnels du client dans mes dossiers que le temps nécessaire à la réalisation des fins identifiées, ou tel que requis ou permis par la loi.

**Choix en matière de confidentialité**

Les clients peuvent demander des copies de mes politiques et procédures de confidentialité à tout moment.

Les clients peuvent demander l’accès à leurs renseignements.  Je dois répondre à cette demande le plus rapidement possible, mais au plus tard 30 jours après la réception de la demande.

Les clients peuvent retirer leur consentement à tout moment en communiquant avec moi en tant que responsable de la protection de la vie privée.  Cependant, ils seront informés que le défaut de fournir des informations adéquates peut m’empêcher de terminer la tâche pour laquelle nous avons été engagés.

Les clients peuvent déposer des plaintes concernant mes procédures de confidentialité ainsi qu’une violation de ma politique de confidentialité.  Les plaintes doivent être reçues par écrit et transmises au responsable de la protection de la vie privée.  Le responsable de la protection de la vie privée communiquera avec le client et obtiendra tous les détails. L’agent de protection de la vie privée examinera ensuite les circonstances de la plainte et déterminera s’il y a lieu de modifier la politique de confidentialité existante. Les compagnies d’assurance devraient être avisées de toute plainte concernant leurs clients ou produits.

**Exception à l’accès client**

Les organisations doivent refuser à une personne l’accès aux renseignements personnels :

* s’il révélerait des renseignements personnels sur une autre personne, à moins qu’il n’y ait consentement ou qu’il y ait une situation mettant sa vie en danger
* si l’organisation a divulgué des renseignements à une institution gouvernementale pour des raisons d’application de la loi ou de sécurité nationale.  Sur demande, l’institution gouvernementale peut demander à l’organisation de refuser l’accès ou de ne pas révéler que les renseignements ont été divulgués.  L’organisation doit refuser la demande et aviser le commissaire à la protection de la vie privée.  L’organisation ne peut pas informer la personne de la divulgation à l’institution gouvernementale, ou que l’institution a été informée de la demande, ou que le commissaire à la protection de la vie privée a été avisé du refus.

Les organisations peuvent refuser l’accès aux renseignements personnels si ces renseignements relèvent de l’un des éléments suivants :

* secret professionnel de l’avocat
* informations commerciales confidentielles
* la divulgation pourrait nuire à la vie ou à la sécurité d’une personne
* il a été recueilli à l’insu ou sans le consentement de la personne pour en assurer la disponibilité et l’exactitude, et le recouvrement a été exigé pour enquêter sur une violation d’une entente ou une contravention à une loi fédérale ou provinciale (le commissaire à la protection de la vie privée doit en être avisé)
* il a été généré au cours d’un processus officiel de règlement des différends.

**Sécurité physique**

* Notre bureau est sécurisé par des serrures et un système d’alarme.
* Personne d’autre que le personnel autorisé n’a accès au bureau.
* Les informations client sont conservées sur site dans des fichiers clients verrouillés dans une armoire.
* Les bureaux sont nettoyés et les dossiers verrouillés à la fin de chaque journée.
* Les documents contenant des renseignements sur les clients qui ne sont plus nécessaires sont détruits à l’aide du déchiqueteur croisé recommandé.
* Lorsqu’un client cesse d’être un client, nous conservons le dossier pendant une période de 15 ans avant de le détruire par déchiquetage.
* Nous veillons toujours à ce que les renseignements personnels ne soient communiqués qu’au titulaire de la police – les conjoints ne peuvent pas obtenir de renseignements sur les politiques de l’autre.

**Sécurité électronique**

* Les renseignements sur les clients sont conservés dans des bases de données sur place et dans des bases de données dotées de systèmes tiers sécurisés approuvés (comme la Financière Manuvie).
* Nos ordinateurs sont protégés par mot de passe; les mots de passe sont changés régulièrement.
* Les Blackberry sont protégés par mot de passe; les mots de passe sont changés régulièrement.
* Les ordinateurs sont toujours enfermés dans le coffre lorsque vous voyagez.

**Tiers**

* Les renseignements sur les clients ne sont pas partagés avec des tiers sans le consentement exprès des clients.

**Atteinte à la vie privée**

* Si nous prenons connaissance d’une atteinte à la vie privée, nous examinerons notre politique de confidentialité et la modifierons au besoin.
* Si nécessaire, le(s) client(s) concerné(s) en sera(nt) ainsi que la compagnie d’assurance.
* Si nécessaire, nous en informerons notre compagnie d’assurance E&O

**Personnel de conseillers**

* Tout le personnel est conscient de notre besoin de protéger les renseignements personnels
* Tous les membres du personnel ont signé un accord de confidentialité
* Le personnel ne discutera pas des affaires en public à l’extérieur du bureau

Tous les membres du personnel et les conseillers ont examiné les mesures de protection mises en place dans notre bureau et confirment qu’ils comprennent l’importance de protéger les renseignements personnels de nos clients.

Daté de \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20XX en \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_> <\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nom

Si quelqu’un a des questions concernant les informations contenues dans cette politique, veuillez contacter :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Responsable de la protection de la vie privée)

**Exemple - Liste de vérification pour les mesures de protection Office**

(Bureaux de conseillers individuels/corporatifs)

Vous trouverez ci-dessous une liste des mesures de protection que vous pouvez mettre en œuvre dans votre bureau. Cette liste de contrôle peut être personnalisée pour répondre aux besoins de votre bureau.

* Les employés doivent lire et reconnaître par écrit qu’ils comprennent et respecteront la politique de confidentialité
* Tous les membres du personnel sont tenus de signer un accord de confidentialité
* Clause de non-responsabilité en matière de confidentialité sur tous les e-mails, fax, etc.
* Tous les documents confidentiels à retirer de la vue (pendant le déjeuner, les pauses, la fin de la journée)
* Aucune information à la vue du public, sur les bureaux
* Aucune discussion sur les dossiers des clients à l’extérieur du bureau
* Ordinateurs/ordinateurs portables à sécuriser lorsqu’ils sont sans surveillance
* Tous les ordinateurs/ordinateurs portables doivent être protégés par mot de passe
* Pas de partage de mots de passe
* Tous les classeurs à verrouiller
* Tous les vieux papiers contenant des renseignements personnels doivent être déchiquetés
* Toute personne, client ou courtier, doit s’identifier par un code de courtier, un numéro de NAS, une date de naissance, etc. pour confirmer son identité.
* Pas de partage des informations des clients avec des parties non autorisées
* Télécopieur à configurer pour conserver les télécopies en mémoire lorsque le bureau est fermé
* Le bureau est verrouillé et les alarmes sont réglées lorsqu’aucun membre du personnel n’est présent ou le week-end
* Toutes les plaintes des clients relatives à la protection de la vie privée doivent être renvoyées au Bureau de la protection de la vie privéer
* Vider le fichier de déchiquetage tous les jours
* Verrouiller le bac de déchiquetage
* Des certificats de destruction sont reçus pour le matériel déchiqueté

**PROCÉDURES D’ATTEINTE À LA VIE PRIVÉE**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Conseiller/Nom de l’entreprise)

**Coordonnées**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(Responsable de la protection de la vie privée)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Adresse)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Numéro de téléphone)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(N° de télécopieur)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Adresse e-mail)

Chez ***(Nom de l’entreprise),*** nous avons la responsabilité de la conservation et de la protection des renseignements personnels que nous recueillons et conservons sur nos employés et nos clients.

Une partie de notre responsabilité consiste à documenter et à signaler toute violation de la vie privée / violation de ces informations personnelles.

**Qu’est-ce qu’une violation?**

Une atteinte à la vie privée est le résultat d’un accès non autorisé à des renseignements personnels, de leur collecte, de leur utilisation ou de leur divulgation.

**Pourquoi devriez-vous aviser les personnes dans certaines circonstances**

Vos clients et employés s’attendent à ce que les entreprises protègent leurs renseignements personnels. Ils veulent être informés des risques pour la vie privée associés à vos pratiques de traitement des renseignements personnels.

**Que faire après avoir découvert une violation**

* **Remplir le formulaire d’incident d’atteinte à la vie privée**
  + Formulaire complet, inclure tous les détails
* **Effectuer une évaluation préliminaire**
  + Contenir la violation
  + Désigner une personne pour commencer l’enquête
  + Notification préliminaire
    - Escalade interne (responsable personnel de la conformité à la vie privée)
* **Évaluer les risques**
  + quels renseignements personnels étaient en cause
  + quelle était la cause et l’étendue de l’atteinte
  + combien de personnes ont été touchées et qui sont-elles
  + quel préjudice pourrait résulter de l’atteinte
* **Aviser toutes les parties concernées**
  + Institution financière
  + Client
  + Police
  + Commissaire à la protection de la vie privée
* **Prévenir les violations futures**
  + Examiner et établir de nouvelles politiques/prodigues/formation (le cas échéant) pour prévenir de futures atteintes à la vie privée

**Liste de contrôle des atteintes à la vie privée**

(Lignes directrices et étapes pour vous aider à produire des rapports)

### Description de l’incident

* Quelle était la date de l’incident?
* Qui l’a découvert ?
* Détails de ce qui s’est passé?

### Étape 1 : Confinement de l’atteinte et évaluation préliminaire

* Avez-vous contenu la violation (récupération d’informations, arrêt du système informatique, verrouillages modifiés)?
* Avez-vous désigné une personne appropriée pour diriger l’enquête initiale?
* Avez-vous déterminé qui doit être informé de l’incident à l’interne et potentiellement à l’externe à cette étape préliminaire?
* L’atteinte semble-t-elle impliquer un vol ou une autre activité criminelle? Dans l’affirmative, la police a-t-elle été avisée?

### Étape 2 : Évaluer les risques associés à l’atteinte à la vie privée

**(i) Quels renseignements personnels étaient en cause?**

* Quels renseignements personnels étaient en cause (nom, adresse, NAS, finances, médicaux)?
* Sous quelle forme se présentait-il (p. ex., dossiers papier, base de données électronique)?
* Quelles mesures de sécurité physiques ou techniques étaient en place au moment de l’incident (serrures, systèmes d’alarme, cryptage, mots de passe, etc.)?

**(ii) Quelle était la cause et l’étendue de l’infraction?**

* Y a-t-il un risque d’atteintes continues ou d’exposition supplémentaire de l’information?
* Les renseignements personnels peuvent-ils être utilisés à des fins frauduleuses ou à d’autres fins?
* L’information a-t-elle été perdue ou volée? S’il a été volé, peut-on déterminer si l’information a été la cible du vol ou non?
* Les renseignements personnels ont-ils été récupérés?
* S’agit-il d’un incident isolé?

**(iii) Qui a été touché par l’atteinte (employés, clients, fournisseurs de services, autres organisations)?**

**(iv) Y a-t-il un préjudice prévisible découlant de la violation?**

* Quel préjudice pourrait résulter de l’atteinte à la vie privée (p. ex., risque pour la sécurité, vol d’identité, perte financière, perte de possibilités d’affaires ou d’emploi, préjudice physique, humiliation, atteinte à la réputation, etc.)?
* Savez-vous qui a reçu l’information et quel est le risque d’accès, d’utilisation ou de divulgation?
* Quel préjudice pourrait résulter de la violation pour l’organisation (p. ex., perte de confiance, perte d’actifs, exposition financière, procédures judiciaires, etc.)
* Quel préjudice pourrait causer au public à la suite de la notification de l’atteinte (p. ex., risque pour la santé publique ou risque pour la sécurité publique)?

### Étape 3 : Notification

**i) Les personnes touchées devraient-elles être avisées?**

* Quelles sont les attentes raisonnables des personnes concernées?
* Quel est le risque de préjudice pour l’individu? Existe-t-il un risque raisonnable de vol d’identité ou de fraude?
* Y a-t-il un risque de préjudice physique? Y a-t-il un risque d’humiliation ou d’atteinte à la réputation de l’individu ?
* Quelles sont les obligations légales et contractuelles de l’organisation?
* Si vous décidez que les personnes touchées n’ont pas besoin d’être avisées, notez vos raisons.

**(ii) Si les personnes touchées doivent être avisées, quand et qui les avisera?**

* Quelle forme de notification utiliserez-vous (p. ex., par téléphone, lettre, courriel ou en personne, site Web, médias, etc.)?
* Qui avisera les personnes touchées? Avez-vous besoin d’impliquer une autre partie?
* Si les autorités chargées de l’application de la loi sont impliquées, la notification doit-elle être retardée pour s’assurer que l’enquête n’est pas compromise?

**(iii) Quoi et qui devrait être inclus dans la notification?**

Selon les circonstances, les avis peuvent inclure certains des éléments suivants, mais veillez à limiter la quantité de renseignements personnels divulgués dans l’avis à ce qui est nécessaire :

* une description des renseignements personnels visés par l’atteinte à la vie privée;
* les coordonnées de votre organisation qui peuvent répondre aux questions ou fournir de plus amples renseignements;
* si votre organisation a avisé le bureau d’un commissaire à la protection de la vie privée;
* Le bureau des commissaires à la protection de la vie privée devrait-il être informé?
* La police ou toute autre partie devrait-elle être informée? Cela peut inclure les assureurs; les organismes professionnels ou autres organismes de réglementation; les sociétés émettrices de cartes de crédit, les institutions financières ou les agences d’évaluation du crédit; d’autres parties internes ou externes telles que des sous-traitants tiers, des unités commerciales internes qui n’ont pas été informées auparavant de l’atteinte à la vie privée

### Étape 4 : Prévention des atteintes futures

* Quelles mesures à court ou à long terme devez-vous prendre pour corriger la situation (p. ex., formation du personnel, examen ou élaboration de politiques, vérification)?

**Formulaire d’incident/de signalement d’atteinte à la vie privée**

|  |  |
| --- | --- |
| Date: |  |
| Nom de la personne qui remplit le formulaire |  |
| Lieu et date de l’incident |  |
| Description de l’incident |  |
| Cause (si elle est connue) |  |
| Personne(s) affectée(s) (client, employé, conseiller,3e partie) |  |
| Type(s) de renseignements personnels en cause |  |
| Brève description des mesures prises pour contenir l’atteinte |  |
| Qui a été avisé (y compris la date de notification) |  |
| Commentaires supplémentaires |  |

**Personnel - Formation sur la protection de la vie privée**

**Sessions de formation et réunions :**

|  |  |  |
| --- | --- | --- |
| **Date** | **Sujet** | **Nom de l’employé** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**­­­­­­­­­**

**Journal d’examen de la politique de confidentialité**

|  |  |  |
| --- | --- | --- |
| **Date de révision** | **Objet mis à jour** | **Nom et titre de l’évaluateur** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |