**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** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |