Au début de votre *Politique de confidentialité*, nous vous suggérons de mettre l’en-tête de votre conseil. Vous pouvez utiliser le modèle suivant :



***Conseil*** (mettre le numéro et le nom)

(mettre l’adresse, le numéro de téléphone)

(mettre le courriel, le lien pour la page WEB et/ou le lien pour la page *Facebook*)

## POLITIQUE DE CONFIDENTIALITÉ

Le 22 septembre 2022, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé* (la « LOI 25 »)3 est entrée en vigueur. La LOI 25 a pour but de moderniser les règles protégeant les renseignements personnels au Québec, afin qu'elles soient mieux adaptées aux nouveaux défis posés par l'environnement numérique et technologique actuel.

La **Commission d’accès à l’information du Québec**, organisme public qui a notamment pour objectif de voir à la bonne application de la LOI 25, peut imposer des sanctions financières importantes aux sociétés, organismes et associations déficientes.

## RENSEIGNEMENT PERSONNEL: *DÉFINITION*

Un renseignement personnel se définit comme celui qui porte sur une personne physique et permet de l’identifier directement ou indirectement (les « RENSEIGNEMENTS »). Il peut prendre la forme de:

* Renseignements d’identification (adresse, numéro de téléphone, sexe, âge, numéro d’assurance sociale, numéro d’assurance maladie, identifiant numérique, etc.);
* Renseignements de santé (dossier médical, diagnostic, consultation d’une professionnelle ou d’un professionnel de la santé, médicament, ordonnance, renseignements sur la cause d’un décès, etc.);
* Renseignements financiers (revenu d’une personne, renseignements relatifs à l’impôt, numéro de compte bancaire, biens possédés, numéros de cartes de crédit, etc.);
* Renseignements relatifs au travail (dossier disciplinaire, motifs d’absence, dates de vacances, salaire, évaluation du rendement, heures d’entrée et de sortie liées au lieu de travail, etc.);
* Renseignements scolaires et relatifs à la formation (inscription à des cours, choix de cours, résultats scolaires, diplômes, curriculum vitæ, etc.); et
* Renseignements relatifs à la situation sociale ou familiale (documents qui attestent l’état civil, le fait qu’une personne ait ou non des enfants ou qu’elle reçoive des prestations d’aide sociale ou de chômage, etc.).

## GÉNÉRALITÉS

Toutes les précautions doivent être prises pour respecter la confidentialité des renseignements personnels recueillis. Plusieurs moyens sont utilisés pour recueillir et transmettre des renseignements personnels :

* + **Lors d’une rencontre personnelle ou autre;**

Lorsqu’une personne se présente pour une rencontre, une entrevue ou des services, la discrétion est de mise. D’abord, il faut s’assurer qu’aucun document confidentiel ne soit à la vue, que votre écran d’ordinateur n’affiche pas de renseignements nominatifs et que la porte du bureau soit fermée, s’il y a lieu. Pour tout situation délicate, assurez- vous qu’une personne vous accompagne.

* + **Les fiches d’inscriptions ou de renseignements (F-100, bénévoles…);**

Dans la mise en place de mesures de sécurité en vue d’assurer la protection des renseignements personnels, vous devez tenir compte, notamment de la sensibilité, de la finalité de l’utilisation, de la quantité et de la répartition des renseignements personnels que vous recevez auprès des personnes dans l’exécution de votre travail.

* + **Le téléphone, le télécopieur;**

Lors d’un échange téléphonique concernant une information particulière, la porte du bureau est fermée. Seules les informations nécessaires et pertinentes sont demandées ou divulguées en conformité avec les lois.

* + **L’ordinateur, le courrier électronique;**

L’écoute des messages de la boîte vocale se fait avec l’écouteur à la main ou avec la porte du bureau fermée si on utilise le mains-libres.

Lors de l’envoi d’un courriel à plusieurs personnes on envoie le tout par copie carbone aveugle (cci) à moins que toutes les personnes du groupe aient donné leur consentement explicite ou implicite que les autres connaissent leur courriel.

À titre d’exemple, les membres du comité exécutif (régie) donnent un consentement implicite à l’effet que les autres membres du groupe connaissent leur adresse.

Lors de l’aménagement de votre bureau, il faut s’assurer que l’écran de l’ordinateur soit positionné de façon à respecter la confidentialité des informations et des données s’y retrouvant ou de fermer votre écran lors de rencontres.

Il est impératif de ne jamais divulguer les mots de passe de notre ordinateur sauf à la personne responsable du système pour des raisons de sécurité.

Lors d’impression de documents contenant des renseignements personnels, ceux-ci doivent être récupérés aussitôt.

* + **Le courrier interne et le courrier postal;**

Pour toute cueillette, utilisation et divulgation d’un RENSEIGNEMENT, la personne de qui on souhaite obtenir l’information doit vous donner au préalable un consentement actif, explicite, informé et spécifique. Ceci implique que vous devez informer cette personne du but de la cueillette, de l’utilisation et de la divulgation du RENSEIGNEMENT et qu’elle doit y consentir par un geste actif et concret. N’oubliez surtout pas que dans le cas **d’un/une jeune de moins de 14 ans**, le consentement du titulaire de l’autorité parentale est requis.

* + **Facebook, Messenger, et tout autre outil lié aux médias sociaux.**

Les outils informatiques ne vous appartiennent pas et leur utilité est uniquement d’ordre professionnel.

## CUEILLETTE

Lorsqu’un RENSEIGNEMENT est recueilli, il faut Limiter la cueillette aux renseignements qui sont nécessaires. Dans l’exécution de vos fonctions, seuls les suivants sont pertinents :

* + Nom, adresse, coordonnées de communications, date de naissance et statuts civils pour les membres.
	+ Nom, adresse, et coordonnées de communications pour les bénévoles;
	+ Les informations nécessaires pour la gestion administrative du personnel, le cas échéant.

Dans l’éventualité où vous devez avoir accès à d’autres renseignements qui vous apparaissent importants, voir à faire autoriser le tout par écrit par la personne gestionnaire des renseignements personnels du Conseil.

Lorsque vous recueillez un RENSEIGNEMENT, vous devez le faire par un moyen où l’information reçue sera écrite. Cela peut se faire au moyen d’un formulaire de format papier ou numérique, ou par courriel.

* + Dans le cas d’un formulaire papier, nous proposons d’utiliser le formulaire TEXTE D’APPROBATION DE CUEILLETTE ET DE PARTAGE DE RENSEIGNEMENTS PERSONNELS, le texte proposé à l’**Annexe I**.
	+ Dans le cas d’un courriel, nous recommandons de recueillir le RENSEIGNEMENT via un formulaire tel que mentionné au point ci-haut. Si cela n’est pas possible, tentez d’obtenir de l’expéditeur/trice qu’il/elle ajoute le texte suggéré à l’**Annexe II** au sein de son message ou qu’il/elle réponde par l’affirmative à un message comme celui suggéré à l’**Annexe III**.
	+ Lorsque vous recueillez un RENSEIGNEMENT par téléphone ou directement dans un courriel, assurez-vous qu’il soit essentiel et dans sa forme la plus brève. Évitez ainsi de prendre des numéros d’assurance sociale ou des informations financières par ces moyens.

Si vous devez conserver le RENSEIGNEMENT en format « papier », il doit être placé sous clé dans vos classeurs ou votre voûte.

Tous les classeurs qui contiennent un RENSEIGNEMENT doivent être barrés lorsque personne n’est sur place.

Dans le cas du format numérique, le RENSEIGNEMENT doit être conservé dans un espace virtuel (nuage / « Cloud ») ou un serveur indépendant sécurisé qui n’est utilisé que par les membres de votre équipe qui ont accès au RENSEIGNEMENT; Aucun RENSEIGNEMENT n’est conservé sur des ordinateurs de travail des membres de l’équipe;

## ACCÈS

## L’accès aux RENSEIGNEMENTS recueillis est limité et contrôlé :

* La personne visée par un acte particulier peut le consulter. La consultation se fait normalement par l’émission de certificat ou d’extrait d’un acte particulier. Notez que des frais peuvent être appliqués.
* Tout employé ou bénévole du Conseil peut évidemment avoir accès aux RENSEIGNEMENTS qui le/la concerne sans autorisation.
* Si un membre autorisé du Conseil doit avoir accès à un RENSEIGNEMENT pour les fins de son travail, il/elle doit éviter :
	+ - De laisser tout RENSEIGNEMENT sur son bureau ou espaces de travail en son absence;
		- D’apporter un RENSEIGNEMENT avec lui/elle à l’extérieur de son travail;
		- De sauvegarder un RENSEIGNEMENT sur son ordinateur ou appareil mobile personnel; et
		- De divulguer un RENSEIGNEMENT à un tiers qui n’a aucune justification de le recevoir.
* Si un membre autorisé externe au Conseil doit avoir accès à un RENSEIGNEMENT pour les fins de son travail, en plus des recommandations indiquées au point précédent, il/elle doit :
	+ - * Signer un registre du type présenté à l’**Annexe IV**;
			* Si possible, uniquement le consulter sur place;
			* Sinon, lui faire parvenir par un moyen électronique sécuritaire (voir point plus bas) et qu’il/elle confirme que le RENSEIGNEMENT sera détruit dès qu’il ne lui est plus nécessaire.

## UTILISATION, DILVUGATION ET TRANSMISSION

Lorsque nous utilisons, divulguons ou transmettons un RENSEIGNEMENT, les procédures suivantes doivent être suivies :

1. L’accès au RENSEIGNEMENT est limité à la personne qui doit y avoir accès (voir Annexe V) pour les fins d’administration ou pour fournir un service à la personne concernée;
2. Aucun RENSEIGNEMENT ne peut être divulgué à un tiers sans le consentement de la personne concernée, sauf dans le cas de :
	* Motif raisonnable de croire qu’il y a un danger imminent de mort ou de blessures graves que la personne pourrait s’infliger (suicide) ou à quelqu’un d’autre (homicide). Nous devons informer les gens susceptibles de lui porter secours ou encore les personnes qui sont exposées au danger;
	* Si l’information reçue porte à croire que la sécurité et/ou le développement d’un mineur sont compromis, la *Loi de la protection de la jeunesse* prévoit l’obligation à signaler immédiatement cette situation au Directeur de la protection de la jeunesse; et
	* Si un juge demande le dossier de la personne concernée.
3. Si un RENSEIGNEMENT doit être divulgué à un tiers, le consentement de la personne concernée doit être obtenu par écrit à l’avance. Le formulaire à l’Annexe VI doit être utilisé pour obtenir le consentement. La divulgation à un tiers doit être pertinente et utile pour l’avancement du dossier de la personne concernée. Mais encore là, faut-il faire preuve de prudence, car des manœuvres frauduleuses peuvent largement être utilisées.
4. Avant de procéder à la divulgation au tiers, celui-ci/celle-ci doit déjà avoir un engagement de confidentialité avec votre organisme ou il/elle doit signer un tel engagement au préalable. Dans ce dernier cas, il faut communiquer avec le/la responsable de la gestion des renseignements personnels pour un document conforme.
5. Tout dossier ou document contenant un RENSEIGNEMENT est transmis via le courrier interne ou la poste.
* En pratique, il n’est pas permis de transmettre un RENSEIGNEMENT par téléphone sur le contenu d’un acte enregistré à moins d’avoir obtenu l’autorisation de la part du Grand Chevalier ou de la personne concernée.
1. Il est strictement interdit de faire des photocopies des registres ou du *Roster,* en tout ou en partie, sauf si la requête provient de la direction de l’État civil ou encore du Conseil d’État ou du Conseil Suprême.
2. Si un RENSEIGNEMENT doit être transmis par un moyen électronique, veuillez-vous assurer que le contenant de l’information soit sécurisé. Ceci peut prendre la forme :
* D’une communication via une application sécurisée, soit un système de courriel sécurisé ou une application de type WhatsApp; ou d’une protection avec mot de passe du document dans lequel se retrouve le RENSEIGNEMENT. Vous trouverez en Annexe VII, des exemples de protection de documents.
* Assurez-vous que l’adresse électronique du destinataire est conforme avant de procéder à la transmission du RENSEIGNEMENT.
1. De façon générale, le télécopieur ne doit pas être utilisé pour la transmission d’un RENSEIGNEMENT si une autre méthode peut satisfaire à la demande.
* Dans l’éventualité où retarder la transmission d’un RENSEIGNEMENT pourrait causer un préjudice, il faut prendre les mesures nécessaires afin que cette transmission soit faite en respectant la confidentialité. Nous devons donc vérifier que les coordonnées du destinataire soient exactes et que celui-ci soit disponible pour la réception de la télécopie.
* Également, nous devons nous assurer que la composition du numéro sur le télécopieur ne comporte pas d’erreur avant de démarrer la transmission.
* L’avis de confirmation doit être conservé au dossier avec la page de transmission.

## DESTRUCTION

## L’autorité supérieure de l’Ordre concernée établit à 100 ans le délai de protection applicable aux RENSEIGNEMENTS, prenant en considération la mise en garde du Barreau du Québec et de la Chambre des notaires contre un délai de prescription trop court, qui ne serait pas soucieux de protéger la famille d’une personne donnée.

## Ce délai permet de protéger les informations privées pendant que la personne vit ; d’autre part, il évite de léser indûment les membres de la famille et les descendants de la personne concernée.

## DEMANDE D’ACCÈS OU DE RECTIFICATION

## Toute demande d’accès ou de rectification d’un RENSEIGNEMENT doit être promptement communiquée à la personne responsable de la gestion des renseignements personnels du Conseil.

## PLAINTES ET INCIDENTS

## Toute plainte, incident ou motif de plainte ou d’incident concernant la gestion des renseignements personnels doit être immédiatement communiqué à la personne responsable de la gestion des renseignements personnels du Conseil. À ce titre, cette personne doit suivre la procédure fournie à l’Annexe VIII, inscrire l’incident au *Registre des incidents* et informer la Commission d’accès à l’information du Québec.

## Un incident peut prendre l’une des formes suivantes :

* Tout accès, utilisation ou divulgation non autorisé d’un RENSEIGNEMENT en vertu de la POLITIQUE;
* La perte d’un RENSEIGNEMENT ou à toute autre atteinte à sa protection;
* Une consultation de RENSEIGNEMENT non autorisée;
* Une divulgation de RENSEIGNEMENT personnel à un mauvais destinataire; ou
* Le Conseil est victime d’une cyberattaque : hameçonnage, rançongiciel, etc.

## SANCTIONS

## À vérifier avec les autorités.

## CONTACT

## Si vous avez des questions concernant la POLITIQUE ou en regard de toute disposition du MANUEL ou de la LOI 25, veuillez communiquer avec

##  Nom

##  Adresse

##  Téléphone

##  courriel

## VERSION

Cette version de la procédure a été mise à jour le 2024.

**DESCRIPTION DES EXIGENCES DE LA LOI 25**

**À partir du 22 septembre 2022 :**

* Désigner une personne responsable de la protection des renseignements personnels et publier le titre et les coordonnées du responsable sur le site Internet de l’entreprise;
* En cas d’incident de confidentialité impliquant un renseignement personnel :
* prendre les mesures raisonnables pour diminuer les risques qu’un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature ne se produisent;
* aviser la Commission d’accès à l’information (la « Commission ») et la personne concernée si l’incident présente un risque de préjudice sérieux; et
* tenir un registre des incidents dont une copie devra être transmise à la Commission à sa demande.
* Respecter le nouvel encadrement de la communication de renseignements personnels sans le consentement de la personne concernée à des fins d’étude, de recherche ou de productions de statistiques et dans le cadre d’une transaction commerciale;
* Procéder à une évaluation des facteurs relatifs à la vie privée (ÉFVP) avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d’étude, de recherche ou de production de statistiques;
* Divulguer préalablement à la Commission la vérification ou la confirmation d'identité faite au moyen de caractéristiques ou de mesures biométriques.

**À partir du 22 septembre 2023 :**

* Avoir établi des politiques et des pratiques encadrant la gouvernance des renseignements personnels et publier de l’information détaillée sur celles-ci en termes simples et clairs sur le site Internet de l’entreprise;
* Réaliser une évaluation des facteurs relatifs à la vie privée (ÉFVP) lorsque la Loi l’exige, par exemple avant de communiquer des renseignements personnels à l’extérieur du Québec;
* Respecter les nouvelles règles entourant le consentement à la collecte, à la communication ou à l’utilisation des renseignements personnels;
* Détruire les renseignements personnels lorsque la finalité de leur collecte est accomplie, ou les anonymiser pour les utiliser à des fins sérieuses et légitimes, sous réserve des conditions et d’un délai de conservation prévus par une loi;
* Respecter vos nouvelles obligations d’information et de transparence envers les citoyens;
* Respecter les nouvelles règles de communication de renseignements personnels sans le consentement de la personne concernée (exercice d’un mandat ou exécution d’un contrat de service ou d’entreprise);
* Respecter les nouvelles règles de communication des renseignements personnels à l'extérieur du Québec;
* Respecter les nouvelles règles d’utilisation des renseignements personnels;
* Prévoir, par défaut, les paramètres assurant le plus haut niveau de confidentialité du produit ou du service technologique offert au public;
* Respecter les nouvelles règles entourant la collecte de renseignements personnels concernant un mineur;
* Respecter le droit à la cessation de la diffusion, à la réindexation ou à la désindexation (ou droit à l'oubli); et
* Respecter les nouvelles règles de communication des renseignements personnels facilitant le processus de deuil.

**À partir du 22 septembre 2024 :**

* Répondre aux demandes de portabilité des renseignements personnels.

# ANNEXE I : Texte de reconnaissance de cueillette de renseignements personnels sur papier :

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

**TEXTE D’APPROBATION DE CUEILLETTE ET DE PARTAGE**

**DE RENSEIGNEMENTS PERSONNELS**

Par la présente, je consens à ce que mes données personnelles écrites sous-dessous soient utilisées et publiées dans le cadre des activités de l’Ordre de Chevaliers de Colomb à tous les niveaux et seulement dans ce cadre (inscrire seulement les RENSEIGNEMENTS désirés).

***FC ;*** # membre

Prénom et nom en lettres moulées Chevalier de Colomb

Date de naissance :

Prénom et nom de la conjointe :

Adresse de résidence :

Courriel :

en lettres moulées minuscules

Téléphone à la résidence. :

Cellulaire :

Consentement signé le

 À

 *Signature*

# ANNEXE II : Texte de reconnaissance de cueillette de renseignements personnels en numérique

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

**TEXTE D’APPROBATION DE CUEILLETTE ET DE PARTAGE**

**DE RENSEIGNEMENTS PERSONNELS**

« Je comprends et accepte que pour les fins énoncées dans notre échange courriel, le Conseil recueille et conserve certains renseignements personnels pertinents (les « RENSEIGNEMENTS ») pour les fins de suivi de mon profil et qu’il pourra les partager avec des tiers pour les fins de rendre le service prévu.

Par conséquent, j’autorise le Conseil à procéder à la cueillette et au partage de mes RENSEIGNEMENTS tel qu’indiqué plus haut. »

Consentement signé le

 À

 *Signature*

# ANNEXE III : Texte de reconnaissance de cueillette de renseignements personnels en numérique

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

**TEXTE D’APPROBATION DE CUEILLETTE ET DE PARTAGE**

**DE RENSEIGNEMENTS PERSONNELS**

« Pour les fins de suivi de votre profil, vous comprenez que le Conseil \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ recueille et conserve certains de vos renseignements personnels pertinents (les « RENSEIGNEMENTS ») et qu’il est possible que nous devions les partager avec des tiers pour les fins de rendre le service prévu.

Par conséquent, nous comprenons que vous autorisez le Conseil \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ à procéder à la cueillette et au partage de vos RENSEIGNEMENTS tel qu’indiqué plus haut. »

Consentement signé le

 À

 *Signature*

# ANNEXE IV : EXEMPLE DE REGISTRE D’ACCÈES

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

## REGISTRE D’ACCÈS À DES RENSEIGNEMENTS PERSONNELS

En tant que Conseil faisant partie de l’Ordre des Chevaliers de Colomb, nous devons assurer que les renseignements personnels que nous gérons demeurent confidentiels selon les modalités de *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé*. Vous comprenez qu’en signant ce registre vous vous engagez à :

* Garder confidentiels les renseignements obtenus et à ne pas les partager à quiconque sans notre autorisation;
* Traiter ces renseignements de façon sécuritaire; et
* Nous retourner la copie originale contenant les renseignements et à détruire toute copie résiduelle, qu’elle soit physique ou numérique.

Nous vous remercions de votre attention à ceci.

|  |  |  |  |
| --- | --- | --- | --- |
| **NOM** | **FONCTION** | **DATE** | **RENSEIGNEMENT OBTENU** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# ANNEXE V : LISTE DE GESTION DES ACCÈS

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

## Liste de gestion des accès dans le Conseil

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Informations** | **Grand Chevalier** | **Secrétaire Financier** | **Secrétaire Archiviste** | **Directeur des programmes** | **\_\_\_\_\_** |
| Nom et prénom |  |  |  |  |  |
| Coordon-nées |  |  |  |  |  |
| Date de naissance |  |  |  |  |  |
| **Informations** | **Directeur général** | **Secrétaire** | **Comptable** | **\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_** |
| Nom et prénom des employés |  |  |  |  |  |
| Coordonnées des employés |  |  |  |  |  |
| Informations financières des employés |  |  |  |  |  |
| Numéro d’assurance sociale des employés |  |  |  |  |  |
| Date de naissance des employés |  |  |  |  |  |

# ANNEXES VI : CONSENTEMENT DE PARTAGE DE RENSEIGNEMENTS PERSONNELS

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

## FORMULAIRE DE CONSENTEMENT DE PARTAGE DE RENSEIGNEMENTS PERSONNELS

Le Conseil détient des renseignements personnels à mon égard pour les fins de me rendre divers services (les « RENSEIGNEMENTS »). Je comprends et accepte que le DÉTENTEUR doit fournir les RENSEIGNEMENTS à

[Nom du tiers externe] (le « TIERS ») pour les fins de

 [Raison du partage d’information].

Je comprends que le TIERS est tenu aux mêmes obligations que le DÉTENTEUR quant à la gestion de mes renseignements personnels ainsi qu’à leur destruction lorsque l’usage par le TIERS n’est plus nécessaire.

Par conséquent, j’autorise le DÉTENTEUR à la transmission des RENSEIGNEMENTS au TIERS.

Consentement signé le

 À

 *Signature*

# ANNEXES VII : EXEMPLES DE PROTECTION DE DOCUMENTS VIRTUELS

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

## EXEMPLES DE PROTECTION DE DOCUMENTS VIRTUEL

**WORD**

1. Cliquez sur « Outils » et choisissez « Protéger le document ».



1. Entrez les informations secrètes.



**PDF**

1. Cliquez sur « Fichier » et choisissez « Protéger à l’aide d’un mot de passe ».



1. Entrez les informations secrètes.



**PAGES**

1. Cliquez sur « Fichier » et choisissez « Définir un mot de passe »



1. Entrez les informations secrètes.



# ANNEXES VIII : PROCÉDURE EN CAS D’INCIDENT DE SÉCURITÉ

Au début de ce document, nous vous suggérons de mettre l’en-tête de votre conseil.

**PROCÉDURE EN CAS D’INCIDENT DE SÉCURITÉ**

\*\* Cette procédure s’adresse à la personne responsable de la gestion des renseignements personnels. \*\*

En cas d’incident, vous devez avoir reçu de la personne qui vous a informée de l’incident les informations suivantes :

* La date et l’heure de l’incident;
* La cause de l’incident
* Les effets de celui-ci
* Le nombre de personnes affectées.

La procédure suivante spécifie les étapes à effectuer lors d’un incident de sécurité dans votre entreprise:

1. Inscrire l’incident à votre registre des incidents de confidentialité des renseignements personnels.
2. Procéder à une enquête interne auprès de la ou des personne(s) qui ont été témoin(s) de l’incident, afin recueillir les informations nécessaires.
3. Évaluer si l’incident de confidentialité pourrait causer un préjudice sérieux aux personnes concernées.
4. Prendre des mesures pour diminuer les risques de préjudice et éviter que des incidents similaires ne se produisent à l'avenir. Dans le cas où l’incident provient du système informatique, discuter avec votre fournisseur de service pour trouver une solution et enrayer la problématique.
5. Aviser la Commission d’accès à l’information d'un incident de confidentialité impliquant un renseignement personnel si l'incident présente un risque sérieux de préjudice en transmettant le formulaire (en pièce jointe) et les documents pertinents par courrier électronique, par la poste ou par télécopieur aux coordonnées suivantes:

**Commission d'accès à l'information**

525, Boulevard René-Lévesque Est, Bur. 2.36 Québec (Qc) G1R 5S9

Téléphone : 418 528-7741 - Sans frais : 1 888 528-7741 - Télécopieur : 418 529-3102 Courrier électronique : cai.communications@cai.gouv.qc.ca

1. Aviser toute personne dont les renseignements personnels ont été compromis par courriel, sans dévoiler l’information exacte, dans le cas où l'incident présente un risque sérieux de préjudice. Toutefois, l’organisation n’a pas à aviser les personnes dont les renseignements personnels sont concernés, si cet avis est susceptible d’entraver une enquête menée en vertu de la loi pour prévenir, détecter, réprimer le crime ou les infractions aux lois.

<https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises>