Société du Centre des congrès de Québec

# PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

**(2022-12-13)**

## 1 OBJET

La présente procédure a pour principal but de déterminer les rôles et les responsabilités en cas d'incidents de confidentialité.

## 2 BUTS

- Déterminer les étapes associées à la gestion d'un incident de confidentialité
- Diminuer les risques qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné, et éviter qu'une situation similaire ne se reproduise.

## 3 CHAMP D'APPLICATION

Tout le personnel de la Société.

La présente procédure s'applique également si un tiers détient des renseignements personnels pour le compte de la Société.

## 4 PRINCIPES GÉNÉRAUX

Dans le respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, la Société met tout en œuvre pour évaluer ou prévenir les risques d'incident de confidentialité.

## 5 RÔLES ET RESPONSABILITÉS

La politique sur la gestion des renseignements personnels (GRI-1) précise les rôles et responsabilités des intervenants en regard de la protection des renseignements personnels.

# 6 DÉFINITION - INCIDENT DE CONFIDENTIALITÉ

Accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

# 7 ÉVALUATION DU PRÉJUDICE

Lors d'un incident de confidentialité, la Société doit évaluer s'il en découle un risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné. Elle doit alors considérer plusieurs facteurs, dont :

- La sensibilité des renseignements personnels, tels un renseignement financier ou un renseignement d'identité;

- Les conséquences appréhendées de l'utilisation de ces renseignements, comme un vol d'identité, une fraude financière, ou une atteinte importante à la vie privée.

- La probabilité que ces renseignements puissent être utilisés à des fins préjudiciables.

Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple :

- À l'humiliation;
- À une atteinte à la réputation;
- À une perte financière;
- À un vol d'identité;
- À des conséquences négatives sur un dossier de crédit;
- À une perte d'emploi.

# 8 PROCÉDURE ADVENANT UN INCIDENT DE CONFIDENTIALITÉ

Les étapes qui suivent peuvent être réalisées simultanément. Celles-ci ne tiennent pas compte des autres règles auxquelles peut être assujettie la Société à titre d'organisme public, par exemple des directives gouvernementales.

1. **Évaluer la situation**. Si un membre du personnel a des raisons de croire que s'est produit un incident de confidentialité impliquant un renseignement, celui-ci doit immédiatement signaler l'incident et aviser le directeur de son unité administrative ainsi que le responsable de l'accès à l'information et de la protection des renseignements personnels.

   Cette personne fournira les informations nécessaires qui contribueront à faire un portrait de la situation, lequel comprendra notamment :

   - Établir les circonstances de l'incident;
   - Identifier les renseignements personnels impliqués;
   - Identifier les personnes concernées;
   - Trouver la problématique, que ce soit une erreur, une vulnérabilité, etc.
     Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

2. **Diminuer les risques.** Le directeur de l'unité administrative concernée doit prendre rapidement les mesures raisonnables qui s'imposent afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux incidents de même nature ne surviennent, par exemple :

   - Cesser la pratique non autorisée;
   - Récupérer ou exiger la destruction des renseignements personnels impliqués;
   - Corriger les lacunes informatiques.

3. **Mobiliser le comité de crise en ressources informationnelles**. Le responsable de l'accès à l'information et de la protection des renseignements personnels mobilise le comité de crise qui est formé des personnes suivantes, et de toute autre ressource dont l'expertise est nécessaire :

   - Responsable des technologies de l'information
   - Responsable du réseau et de la sécurité de l'information
   - Technicien en informatique
   - Directeur de l'administration
   - Secrétaire générale (responsable de l'accès à l'information et de la protection des renseignements personnels)

   Par la suite, chaque membre du comité s'assure de la disponibilité des ressources qui participeront à la gestion de l'incident.

4. **Identifier la nature du préjudice,** afin de déterminer s'il faut aviser la Commission d'accès à l'information (CAI) et les personnes concernées et, aussi, afin d'établir les mesures à mettre en place pour diminuer les risques.

   Cette évaluation se fait selon les principes et les facteurs identifiés au paragraphe 7.

5. **Inscrire l'incident au registre**, que le risque de préjudice soit qualifié ou non de sérieux et **inscrire une note dans les dossiers visés** par un risque de vol d'identité.

6. **S'il y a un risque de préjudice sérieux,** la Société doit :

   - **Aviser la CAI dès que possible**, même si l'ensemble des informations relatives à l'incident ne sont pas colligées, et remplir la déclaration par la suite. Ainsi, la CAI sera avisée de l'incident et, plus tard, le nombre de personnes concernées pourra être confirmé.

   - **Aviser toute personne dont un renseignement personnel est concerné par l'incident**, à moins que cet avis ne soit susceptible d'entraver une enquête. Un délai peut s'appliquer entre le moment où il y aura prise de connaissance de l'incident et celui où les personnes concernées seront avisées. Ce délai peut être nécessaire afin, par exemple, d'identifier les renseignements personnels impliqués, les personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

     *Ces deux premiers avis sont obligatoires. Toute décision de ne pas aviser la CAI et les personnes concernées devrait être documentée, incluant les motifs à l'origine de cette décision.*

   - **Aviser l'équipe de gestion des incidents (CERT/AQ)** du Centre gouvernemental de cyberdéfense (CGCD) du ministère de la Cybersécurité et du Numérique.

- **Aviser les services policiers si un crime semble avoir été commis**.

- **Aviser ses assureurs**.

- **Aviser les conseillers juridiques** pour obtenir des conseils relativement à la préservation de la preuve et aux risques juridiques associés aux mesures déployées.

- **La Société peut aussi aviser toute personne ou tout organisme susceptible de diminuer ce risque.** À cette fin, elle ne peut lui communiquer que les renseignements personnels qui sont nécessaires à la poursuite de cet objectif. L'obtention du consentement de la personne concernée par les renseignements transmis n'est pas requise. Toutefois, la personne responsable d'accès à l'information et de la protection des renseignements personnels doit enregistrer la communication pour garder des traces documentaires de celle-ci comme :

  - À qui ces renseignements sont communiqués;
  - Dans quelles circonstances;
  - Quels renseignements ont été transmis;
  - Quels sont les objectifs de cette démarche.

7. **Assurer un suivi et l'amélioration du processus de gestion** auprès de tous les intervenants. Documenter la gestion de l'incident, revoir les contrôles défaillants et établir un plan d'action.

## 9 MESURES À L'ÉGARD DES PERSONNES VICTIMES DU BRIS DE CONFIDENTIALITÉ

Dans l'éventualité où une personne serait victime d'un incident de confidentialité, les membres du comité de crise identifieront une personne qui agira à titre de contact auprès des victimes. En fonction de la situation, celle-ci les informera des mesures qui seront mises en place afin d'atténuer les risques de préjudice. Des mesures que les victimes pourront prendre elle-mêmes seront également suggérées.

## 10 TENUE D'UN REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le responsable de la protection des renseignements personnels doit tenir un registre de l'ensemble des incidents de confidentialité dont la Société a fait l'objet, même de ceux qui ne présentent pas un risque de préjudice sérieux pour les personnes.