# Procédure de gestion des incidents de confidentialité

Juin 2023

# TABLE DES MATIÈRES

# PRÉAMBULE

Selon la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre p-39.1), un « incident de confidentialité » survient lors de :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Depuis le 22 septembre 2022, les organisations assument de nouvelles obligations concernant le traitement des incidents de confidentialité. Ces obligations visent à garantir un suivi adéquat et diligent des organisations lorsque survient un tel événement. À cet effet, les organisations doivent notamment tenir un registre des incidents de confidentialité.

La présente procédure vise donc à détailler les marches à suivre en cas d'incident de confidentialité.

Les obligations varient selon la gravité de l'événement. La présente procédure détaille donc les marches à suivre :

- En toutes circonstances;
- Lorsque l'incident présente un risque qu'un préjudice sérieux soit causé.

## Portée

Cette procédure couvre tout incident de confidentialité touchant l'information que possède le FIQ – Syndicat des professionnelles en soins de la Capitale-Nationale (ci-après, « le Syndicat »).

## Responsable de la procédure

La responsable de la protection des renseignements personnels du Syndicat est responsable de l'application et du respect de cette procédure.

# REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Les organisations doivent tenir un registre des incidents de confidentialité. Il s'agit d'une obligation fondamentale pour répertorier les événements qui se sont produits dans l'organisation et s'assurer qu'un suivi soit fait avec diligence.

Le registre documente tous les incidents de confidentialité qui sont survenus au Syndicat.

## Forme du registre

Le Syndicat tient un registre structuré en format numérique pour documenter chaque incident de confidentialité.

Le registre des incidents se compose de plusieurs sous-dossiers propres à chaque nouvel incident de confidentialité. Ainsi, pour chaque nouvel incident, on retrouve :

- Extrait du registre des incidents de confidentialité (Annexe 1);
- Notes évolutives sur la gestion de l'incident (Annexe 2);
- Formulaire d'avis à la Commission d'accès à l'information, au besoin (Annexe 3);
- Lettre d'avis à la personne concernée par l'incident de confidentialité, au besoin (Annexe 4);

La tenue de ce registre est faite avec diligence et les mesures de suivi y sont inscrites sous forme de notes évolutives. Par ailleurs, une copie du registre doit être transmise à la Commission d'accès à l'information (CAI) si elle en fait la demande.

## Contenu du registre

Conformément au Règlement sur les incidents de confidentialité, entré en vigueur le 29 décembre 2022, le Registre des incidents de confidentialité doit contenir les renseignements suivants :

1° une **description des renseignements personnels visés** par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

2° une brève description des **circonstances de l'incident**;

3° la **date ou la période où l'incident a eu lieu** ou, si cette dernière n'est pas connue, une approximation de cette période;

4° la date ou la période au cours de laquelle l'organisation a **pris connaissance** de l'incident;

5° le **nombre de personnes concernées** par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;

6° une description des **éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux** soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

7° si l'incident présente un risque qu'un préjudice sérieux soit causé, **les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées**, en application du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé, de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;

8° une brève description des **mesures prises par l'organisation**, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

### Durée de conservation du registre

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant **une période minimale de cinq ans** après la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.

## ÉTAPES À SUIVRE

### En toutes circonstances

Le Syndicat doit faire preuve de diligence dès le constat d'un incident de confidentialité.

À cet effet, une prise en charge adéquate et l'implantation de mesures de mitigation s'imposent dès les premiers instants. Cette gestion de la situation permettra ensuite de faire un examen plus approfondi et d'évaluer plus en détail le risque qu'un préjudice sérieux ait pu être causé aux personnes concernées.

Une fois que la situation est maîtrisée, il demeure essentiel d'assurer un suivi de manière qu'un événement de même nature ne puisse se reproduire.

### *ÉTAPE 1 : Désigner une personne responsable de la gestion de la situation*

Par défaut, la responsable de la protection des renseignements personnels est responsable de la gestion de l'incident. Elle doit donc être avisée en premier lieu dès que l'on constate qu'il s'est produit un incident de confidentialité.

La responsable de la protection des renseignements personnels peut toutefois désigner une personne responsable de la gestion de la situation. Cette personne peut être une personne désignée au sein de l'organisation, selon le secteur impliqué, ou simplement celle qui a détecté l'incident.

La personne responsable de la gestion de la situation devra :

- Prendre en charge la gestion de l'incident de confidentialité;
- Assurer un suivi des mesures prises afin de mitiger les dommages;
- Documenter le traitement de l'incident de confidentialité avec diligence;
- Répondre aux demandes concernant l'événement.

En tout temps, la personne responsable de la gestion de la situation devra rendre des comptes à la responsable de la protection des renseignements personnels.

### *ÉTAPE 2 : Faire une évaluation préliminaire de la situation*

Dès les premiers instants, la personne responsable doit procéder à une analyse préliminaire de la situation lorsqu'on a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel s'est produit. Il s'agit alors d'identifier :

- La nature de l'incident;
- Les renseignements personnels concernés;
- Le support concerné (papier, électronique, clé USB, etc.);
- L'estimation du nombre de personnes visées;
- Les circonstances de l'événement;
- Etc.

Cette évaluation préliminaire permettra d'évaluer la gravité de l'événement et de prendre les mesures appropriées pour diminuer le risque. Ces informations seront ensuite consignées à l'extrait du registre concernant l'incident (Annexe 1).

### *ÉTAPE 3 : Adopter des mesures de mitigation*

Une fois que l'événement a bien été identifié, le Syndicat doit prendre sans tarder les mesures raisonnables pour en limiter les conséquences négatives et éviter qu'un nouvel incident de même nature ne se produise.

À cet effet, la responsable de la gestion de l'incident doit notamment :

1. **Mettre fin** à la pratique non conforme, le cas échéant, et prendre des mesures afin de limiter immédiatement les conséquences d'une perte ou d'un vol de renseignements personnels;
2. **Récupérer** les dossiers physiques ou numériques, selon le cas;
3. **Révoquer ou modifier** les mots de passe ou les codes d'accès informatiques;
4. **Contrôler** les lacunes dans les systèmes de sécurité.

### *ÉTAPE 4 : Évaluer les risques de préjudice*

Une fois que ces mesures correctrices ont été adoptées, la responsable de la gestion de l'incident doit faire une évaluation complète des risques qu'un préjudice soit causé en raison de l'incident de confidentialité.

La personne responsable pourra consulter les outils d'évaluation du risque de préjudice sérieux (Annexe 5). Ce système permet de catégoriser l'importance des événements et de faciliter l'analyse. Or, lorsqu'elle évalue le risque qu'un préjudice soit causé, la personne responsable de la gestion de l'incident, de concert avec la responsable de la protection des renseignements personnels, **doit considérer**, notamment :

- la sensibilité du renseignement concerné;
- les conséquences appréhendées de son utilisation;
- la probabilité qu'il soit utilisé à des fins préjudiciables.

**Définition :** Renseignement personnel sensible

Aux fins de l'analyse, on considère qu'un renseignement personnel est **«** sensible **»** lorsque, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

Exemples :
Dossier médical, avis disciplinaire, numéro d'assurance sociale, etc.

Advenant que l'évaluation démontre que l'incident présente un risque de préjudice sérieux, des actions supplémentaires devront être prises par l'organisation (voir aux étapes 7 et 8).

### *ÉTAPE 5 : Tenue du Registre des incidents de confidentialité*

Comme indiqué précédemment, les organisations doivent tenir un registre des incidents de confidentialité. Il s'agit d'une obligation fondamentale pour assurer le suivi et répertorier tous les événements qui se sont produits dans l'organisation.

À cet effet, la responsable de la gestion de l'incident doit :

- Remplir l'extrait du registre en lien avec l'événement (Annexe 1);
- Transmettre l'information à la responsable de la protection des renseignements personnels.

La responsable de la protection des renseignements personnels est responsable de la tenue du registre. À cet effet, pour centraliser l'ensemble des incidents au sein d'un même registre, elle devra créer un nouveau sous-dossier propre à chaque nouvel incident. Elle devra ensuite y verser l'ensemble des documents pertinents en lien avec la gestion de l'événement (extrait du registre, notes évolutives et, au besoin, les avis envoyés à la Commission d'accès à l'information et aux personnes concernées).

Une copie du registre doit être transmise à la Commission d'accès à l'information (CAI) si elle en fait la demande.

### *ÉTAPE 6 : Suivi*

Dans une optique d'amélioration continue, la personne responsable de la gestion de l'incident effectue le suivi :

- du processus de traitement qui doit être appliqué lors d'une perte ou d'un vol de renseignements personnels et des résultats obtenus afin de l'améliorer, s'il y a lieu;
- des mesures de sécurité requises à la suite de l'incident et de leur performance;
- de la communication de l'information pertinente à la Commission d'accès à l'information et au service de police impliqué, le cas échéant.

La personne responsable de la gestion de l'incident documente les mesures de suivi sous forme de notes évolutives (Annexe 2). Régulièrement, ces notes sont transmises à la responsable de la protection des renseignements personnels pour mettre à jour le sous-dossier concernant la gestion de l'événement dans le Registre des incidents de confidentialité.

## Lorsque l'incident présente un risque de préjudice sérieux

Une évaluation du risque a déjà été produite à l'étape 4. À cet effet, en plus de l'adoption de mesures correctrices et la tenue du registre des incidents, certaines obligations pourraient s'ajouter au terme de l'analyse.

En effet, l'organisation sera tenue d'aviser la Commission d'accès à l'information (CAI) et la personne concernée si l'évaluation conclut que l'incident présente un risque de préjudice sérieux.

### *ÉTAPE 7 : Avis à la Commission d'accès à l'information*

Si l'incident présente un risque qu'un préjudice sérieux soit causé, le Syndicat doit, avec diligence, aviser la Commission d'accès à l'information (CAI).

#### Délai de transmission

L'avis à la Commission doit être transmis avec diligence, dans un délai maximal de 30 jours après le constat de l'événement.

#### Contenu de l'avis

Conformément l'article 3 du Règlement sur les incidents de confidentialité, entré en vigueur le 29 décembre 2022, l'avis à la Commission d'accès à l'information est fait **par écrit** et doit répertorier les informations citées au modèle disponible à l'**Annexe 3**.

Une fois complété, le formulaire doit être transmis 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

#### Information postérieure à l'envoi de l'avis

Il est important d'agir avec diligence dans le traitement d'un incident de confidentialité portant un risque de préjudice sérieux. Ainsi, le Syndicat doit transmettre à la Commission d'accès à l'information tout renseignement additionnel dont il prend connaissance après la transmission de l'avis initial. Ces informations complémentaires doivent être transmises avec diligence dès qu'elles sont connues.

### *ÉTAPE 8 : Avis aux personnes concernées*

Si l'incident présente un risque qu'un préjudice sérieux soit causé, le Syndicat doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire.

**Délai de transmission**

L'avis aux personnes concernées doit être transmis avec diligence, dans un délai maximal de 30 jours après le constat de l'événement.

**Contenu de l'avis** (voir le modèle d'avis à l'Annexe 4)

Conformément à l'article 5 du Règlement sur les incidents de confidentialité, entré en vigueur le 29 décembre 2022, l'avis à la personne dont un renseignement personnel est concerné par un incident qui présente un risque qu'un préjudice sérieux soit causé doit contenir les renseignements suivants :

1° une **description des renseignements personnels visés** par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

2° une brève description des **circonstances de l'incident**;

3° la **date ou la période où l'incident a eu lieu** ou, si cette dernière n'est pas connue, une approximation de cette période;

4° une brève description des **mesures que l'organisation a prises** ou entend prendre à la suite de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

5° les **mesures que l'organisation suggère** à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;

6° les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

**Possibilité de transmission par avis public**

En règle générale, l'avis est directement transmis à la personne concernée par l'incident de confidentialité. Toutefois, l'avis peut être donné au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes :

1° lorsque le fait de transmettre l'avis est susceptible de causer un **préjudice accru** à la personne concernée;

2° lorsque le fait de transmettre l'avis est susceptible de représenter une **difficulté excessive pour l'organisation**;

3° lorsque **l'organisation n'a pas les coordonnées** de la personne concernée.

Par ailleurs, l'avis peut également être donné au moyen d'un avis public afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice. Dans ce cas, l'organisation demeure toutefois tenue de transmettre, avec diligence, un avis à la personne concernée.

--

Une fois ces étapes complétées, revenir à l'**étape 6** pour assurer un suivi adéquat de la situation.

## RÉFÉRENCES

- Loi sur la protection des renseignements personnels dans le secteur privé [texte de loi officiel] (Publications Québec)
- Loi sur la protection des renseignements personnels dans le secteur privé [version administrative] (Commission d'accès à l'information du Québec)
- Règlement sur les incidents de confidentialité (Gazette officielle du Québec)
- AIDE-MÉMOIRE À L'INTENTION DES ORGANISMES ET DES ENTREPRISES - QUOI FAIRE EN CAS DE PERTE OU DE VOL DE RENSEIGNEMENTS PERSONNELS? (Commission d'accès à l'information du Québec)

## Annexe 1 Registre des incidents de confidentialité

Une nouvelle fiche doit être créée pour documenter un nouvel incident de confidentialité.

La tenue de ce registre doit être faite avec diligence dès le constat de l'incident. Le suivi du traitement de l'événement doit ensuite y être inscrit sous forme de notes évolutives (Annexe 2).

Une copie doit être transmise à la Commission d'accès à l'information (CAI) si elle en fait la demande.

--

| ***REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ*** | |
|---|---|
| ***Numéro de l'incident*** | *[COMPLÉTER]* |
| ***Renseignements visés par l'incident*** | *Décrire les renseignements personnels visés par l'incident ou en dresser une liste. Si cette information n'est pas connue, il faut le préciser et expliquer la raison qui justifie l'impossibilité de fournir une telle description.*<br>*[COMPLÉTER]* |
| ***Circonstances de l'incident*** | *Décrire brièvement les circonstances de l'incident et, si elle est connue, sa cause.*<br>*[COMPLÉTER]* |
| ***Date ou période de l'incident*** | *Mentionner la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation.*<br>*[COMPLÉTER]* |
| ***Date ou période de la prise de connaissance de l'incident*** | *Mentionner la date ou la période au cours de laquelle le Syndicat a pris connaissance de l'incident.*<br>*[COMPLÉTER]* |
| ***Nombre de personnes concernées par l'incident*** | *Mentionner le nombre de personnes concernées par l'incident ou, si ce dernier n'est pas connu, une approximation.*<br>*[COMPLÉTER]* |
| ***Risque qu'un préjudice sérieux soit causé*** | • *OUI* • *NON*<br><br>*Décrire les éléments qui amènent le Syndicat à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées.*<br>*[COMPLÉTER]* |

Commenté [MPGH1]: Je reprends les mêmes corrections que dans l'exercice. À valider.

| | |
|---|---|
| ***Transmission des avis à la Commission d'accès à l'information et aux personnes concernées*** | ***Date(s) de l'avis à la Commission d'accès à l'information*** *:*<br>*S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates de transmission d'avis. Sinon, inscrire « Sans objet ».*<br>*[COMPLÉTER]*<br><br>***Dates(s) de l'avis aux personnes concernées*** *: [date]*<br><br>***Avis public*** *:* • *OUI* • *NON*<br><br>***Raison*** *:*<br>*Si un avis public a été diffusé, en expliquer la raison. Dans le cas contraire, inscrire « Sans objet ».*<br>*[COMPLÉTER]* |
| ***Description des mesures prises par le Syndicat pour diminuer les risques*** | *Décrire brièvement les mesures prises par le Syndicat, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.*<br>*[COMPLÉTER]* |

## Annexe 2 Notes évolutives sur la gestion de l'incident

Le suivi des actions prises en lien avec l'incident est inscrit sous forme de notes évolutives.

Un nouveau document doit être créé pour documenter chaque nouvel incident de confidentialité. Ce document s'ajoute ensuite au sous-dossier propre à l'incident à l'intérieur du registre.

--

**NOTES ÉVOLUTIVES**

Numéro de l'incident : [à remplir par la *RPRP*]

Date ou période de l'incident :

Responsable de la gestion de la situation :

| Date | Suivi |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## Annexe 3 Modèle d'avis à la Commission d'accès à l'information

Cet avis doit être envoyé à la Commission d'accès à l'information seulement s'il existe un risque de préjudice sérieux aux personnes concernées par l'incident de confidentialité.

Une fois complété, le formulaire doit être transmis 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

--

Bonjour,

En respect de l'article 3 du Règlement sur les incidents de confidentialité, le FIQ – Syndicat des professionnelles en soins de la Capitale-Nationale souhaite vous aviser de la survenance récente d'un incident de confidentialité qui présente un risque qu'un préjudice sérieux soit causé.

Voici les détails de l'incident :

| | |
|---|---|
| ***Nom et adresse de l'organisation*** | FIQ – Syndicat des professionnelles en soins de la Capitale-Nationale<br>*Numéro d'entreprise du Québec (NEQ) : 1172789118*<br><br>*2601 Chemin de la Canardière,*<br>*Québec (Québec) G1J 2G3* |
| ***Renseignements visés par l'incident*** | *Décrire les renseignements personnels visés par l'incident ou en dresser une liste. Si cette information n'est pas connue, il faut le préciser et expliquer la raison qui justifie l'impossibilité de fournir une telle description.)*<br>*[COMPLÉTER]* |
| ***Circonstances de l'incident*** | *Décrire brièvement les circonstances de l'incident et, si elle est connue, sa cause.*<br>*[COMPLÉTER]* |

| | |
|---|---|
| ***Date ou période de l'incident*** | *Mentionner la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation.*<br>*[COMPLÉTER]* |
| ***Date ou période de la prise de connaissance de l'incident*** | *Mentionner la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.*<br>*[COMPLÉTER]* |
| ***Nombre de personnes concernées par l'incident*** | *Mentionner le nombre de personnes concernées par l'incident ou, si ce dernier n'est pas connu, une approximation.*<br>*[COMPLÉTER]* |
| ***Risque qu'un préjudice sérieux soit causé*** | *Décrire les éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées.*<br>*[COMPLÉTER]* |
| ***Description des mesures que l'organisation a prises ou entend prendre pour aviser les personnes concernées*** | *Dates(s) de l'avis aux personnes concernées : [date]*<br><br>*Avis public :* • *OUI* • *NON*<br><br>*<u>Raison</u> :*<br>*Si un avis public a été diffusé, en expliquer la raison. Dans le cas contraire, inscrire « Sans objet ».*<br>*[COMPLÉTER]* |
| ***Description des mesures prises par l'organisation pour diminuer les risques*** | *Décrire brièvement les mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.*<br>*[COMPLÉTER]* |

Pour toute question ou précision complémentaire en lien avec cet événement en particulier, nous vous invitons à communiquer avec [inscrire les coordonnées qui permettront à la Commission d'obtenir des informations supplémentaires relatives à l'incident].

Cordialement,

## Annexe 4 Modèle d'avis à la personne concernée par un incident de confidentialité

Cet avis doit être envoyé à la personne concernée par l'incident de confidentialité seulement s'il existe un risque qu'elle en subisse un préjudice sérieux.

--

[Madame / Monsieur XXX]

Dans le respect des obligations auxquelles elle est tenue en application de la Loi sur la protection des renseignements personnels dans le secteur privé, le FIQ – Syndicat des professionnelles en soin de la Capitale-Nationale souhaite vous informer de la survenance récente d'un incident de confidentialité qui concerne vos renseignements personnels. [Décrire les renseignements personnels visés par l'incident (ex. : Les renseignements personnels visés dans cet incident sont…) ou, si cette information n'est pas connue, la raison qui justifie l'impossibilité de les mentionner].

En effet, [insérer une brève description des circonstances de l'événement]. Cet incident est survenu [inscrire la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période].

Soyez [assurée ou assuré] que nous mettons actuellement en œuvre des mesures afin de diminuer les risques qu'un préjudice vous soit causé. À cet égard, [inscrire une brève description des mesures qui ont été prises ou qui seront prises, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé].

De plus, afin d'optimiser la protection de vos renseignements personnels, nous vous suggérons [décrire les mesures suggérées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer un tel préjudice].

Pour toute question ou précision en lien avec cet événement en particulier, nous vous invitons à communiquer avec [inscrire les coordonnées qui permettront aux personnes concernées d'obtenir des informations supplémentaires relatives à l'incident].

Cordialement,

## Annexe 5 Outils d'évaluation du risque de préjudice sérieux à la personne concernée

| Cote | Nom | Définition<br>(nature, gravité, caractère répétitif, accessibilité,<br>durée du manquement, sensibilité, nombre de personnes concernées) | Sensibilité du renseignement personnel concerné | La protection des renseignements personnels et de la vie privée est-elle compromise ? |
|---|---|---|---|---|
| **1** | Bas<br>Impact négligeable | Une ou plusieurs personnes concernées<br>Le renseignement personnel suscite très peu d'attentes de la personne concernée quant à sa confidentialité.<br>Peu de personnes y ont eu accès.<br>Le renseignement personnel a été récupéré et sécurisé.<br>Des mesures correctives ont été rapidement mises en place. | Aucune sensibilité | Oui, mais c'est un renseignement personnel peu sensible |
| **2** | Moyen<br>Impact modéré | Une ou plusieurs personnes concernées<br>Le renseignement personnel suscite peu d'attentes de la personne concernée quant à sa confidentialité.<br>Plusieurs personnes y ont eu accès.<br>Le renseignement personnel a été récupéré et sécurisé.<br>Ce n'est pas la première fois qu'un incident s'applique dans une installation en particulier ou c'est la même personne qui est à l'origine de l'incident.<br>Des mesures correctives ont été rapidement mises en place (formation, encadrement additionnel). | Faible sensibilité | Oui, mais c'est un renseignement personnel peu sensible |
| **3** | Élevé<br>Impact grave | Une ou plusieurs personnes concernées<br>Le renseignement personnel suscite beaucoup d'attentes de la personne concernée quant à sa confidentialité.<br>Plusieurs personnes y ont eu accès.<br>Le renseignement personnel n'a pas été récupéré, ou, s'il a été récupéré, il est possible que des copies soient en circulation (incident lié à l'infonuagique – extérieur au Syndicat).<br>L'événement pourrait avoir des incidences sérieuses sur les personnes concernées. | Grande sensibilité | Oui, possiblement |
| **4** | Très élevé<br>Impact très grave | Une ou plusieurs personnes concernées<br>Le renseignement personnel suscite énormément d'attentes de la personne concernée quant à sa confidentialité.<br>Plusieurs personnes y ont eu accès<br>Le renseignement personnel n'a pas été récupéré et il est irrécupérable (vol d'un serveur, d'un ordinateur, etc.).<br>L'événement pourrait avoir des incidences extrêmement sérieuses sur les personnes concernées. | Très grande sensibilité | Oui, probablement |