**PROVINCE DE QUÉBEC**

**MUNICIPALITÉ DE SAINTE-SOPHIE-DE-LÉVRARD**

**MRC DE BÉCANCOUR**

# POLITIQUE DE PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

**Adoptée par le conseil municipal le 19 septembre 2023**
**Résolution n° 6467, 09-2023**

**PROVINCE DE QUÉBEC**

**MUNICIPALITÉ DE SAINTE-SOPHIE-DE-LÉVRARD**

**MRC DE BÉCANCOUR**

---

## POLITIQUE DE PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

---

**SÉANCE** extraordinaire du conseil municipal de la Municipalité de Sainte-Sophie-de-Lévrard, tenue le 19 septembre 2023, à 19 h 30, à l'endroit ordinaire des réunions du conseil, soit au 174 St-Antoine, à Ste-Sophie-de-Lévrard, à laquelle séance étaient présents :

**LE MAIRE :** Jean-Guy Beaudet

**LES MEMBRES DU CONSEIL :**

VANESSA ROBIDAS-GRAVEL
JACQUELINE M. LAMBERT
SYLVIE LAMBERT
MARIO DEMERS
PATRICE VAUGEOIS
NANCY C. DEMERS

Tous membres du conseil et formant quorum.

**CONSIDÉRANT QUE** le projet de loi n$^{o}$ 64[1], *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels,* L. Q. c. 25, a été sanctionné ;

**CONSIDÉRANT QU'**à la suite de cette sanction et conformément *à l'article 63.4 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) ) [ci-après : Loi 25] ;

**CONSIDÉRANT** que la municipalité reconnaît l'importance de protéger les renseignements personnels qu'elle détient et met donc en œuvre les moyens technologiques et administratifs nécessaires afin que ceux-ci soient correctement traités tout au long de leur cycle de vie;

**CONSIDÉRANT** qu'une telle politique doit être publiée sur le site Internet de la Municipalité et diffusée par tout moyen propre à atteindre toute personne concernée ;

**EN CONSÉQUENCE, LE CONSEIL DÉCRÈTE CE QUI SUIT :**

## CHAPITRE I - INTERPRÉTATION ET OBJECTIFS

### 1. Définitions

**Aux fins de la présente politique, les expressions ou les termes suivants ont la signification ci-dessous énoncée :**

**CAI :** Désigne la Commission d'accès à l'information créée en vertu de la *Loi sur l'accès*.

**Conseil :** Désigne le conseil municipal de la Municipalité de Sainte-Sophie-de-Lévrard.

**Employé :** Désigne un élu(e), un cadre ou un employé, à temps plein ou temps partiel, permanent, saisonnier ou contractuel.

**Incident de confidentialité :** Désigne l'accès, l'utilisation ou la communication non autorisés par la *Loi sur l'accès* de tout renseignement personnel, sa **PERTE** ou toute autre atteinte à la protection d'un tel renseignement.

**Loi sur l'accès :** Désigne la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A -2,1.

**Personne concernée :** Désigne toute personne physique pour laquelle la Municipalité collecte, détient, communique à un tiers, détruit ou rend anonyme, un ou des renseignements personnels.

**Renseignement personnel (RP) :** Désigne tout renseignements personnels qui concerne une personne physique et qui permet de l'identifier directement ou indirectement. Le nom d'une personne, pris isolément, n'est pas un renseignement personnel. Cependant, lorsque ce nom est associé ou jumelé à un autre renseignement visant cette même personne, il devient alors un renseignement personnel.

Voici des exemples de catégories de renseignements personnels :

- **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.
- **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'assurance-emploi, etc.

Les renseignements personnels sont confidentiels, sauf dans les cas prévus par la Loi. Ils doivent être protégés

conformément à la Loi.
**Responsable de la protection des renseignements personnels (RPRP)** : Désigne la personne de veiller à la conformité des règles et des obligations en matière de protection des renseignements personnels au sein de la municipalité.

**Responsable de l'application**
Le RPRP est responsable de voir à l'application de la présente procédure. Dans le cadre de ses fonctions il peut se faire assister d'autres employés de la Municipalité. Il peut également, sous réserve des règles de gestion contractuelles et de délégation de pouvoir, utiliser des services externes spécialisés en la matière.

Tous les employés doivent collaborer avec le RPRP dans le cadre de l'application de la présente procédure.

## 2. Objectifs de la politique

La Politique de procédure des incidents de confidentialité vise les objectifs suivants :

- Décrire les exigences à respecter
- Identifier les mesures à prendre en cas d'incident de confidentialité
- Définir les rôles et responsabilités des parties prenantes

le tout en conformité avec *les articles 63.8 à 63.11* de la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels* (RLRQ, c. A-2.1).

## CHAPITRE II - COLLECTE DE RENSEIGNEMENTS PERSONNELS ET CONSENTEMENT

## 3. Application de la politique d'incident de confidentialité

La présente politique s'applique à tous les membres du personnel de la municipalité ayant connaissance d'un incident de confidentialité impliquant des renseignements personnels traités au sein de la municipalité ainsi qu'aux tiers traitant des renseignements personnels pour le compte de la municipalité et ayant connaissance d'un incident de confidentialité relatif à ces renseignements doit aviser sans délai la directrice générale et greffière-trésorière soit par courriel au municipalite@ste-sophie-de-levrard.com ou par téléphone au 819 288-5804.

## 4. Processus de traitement d'un incident de confidentialité

Afin de comprendre le processus de traitement d'un incident de confidentialité, une schématisation du processus est jointe à **l'ANNEXE I.**

**Signalement d'un incident de confidentialité**

Les membres du personnel de la municipalité et les tiers signalent, sans délai, à la personne responsable de la protection des renseignements personnels soit à la directrice générale et greffière tout incident ou suspicion d'incident de confidentialité dont ils ont connaissance.

**Exemples d'incidents de confidentialité :**

4.1 Communication par erreur des renseignements personnels à un mauvais destinataire;

4.2 Un vol de dossier ou de données au moyen de divers moyens technologiques (clé USB, piratage, etc.);

4.3 Accès à des renseignements personnels par une personne non autorisée.

Lorsque cela est possible, l'auteur du signalement prend au plus vite les mesures adéquates afin de contenir l'incident et d'en limiter les torts ou dommages.

La personne qui signale l'incident doit indiquer les informations nécessaires pour analyser adéquatement l'incident, en remplissant la fiche d'incident contenue à l'ANNEXE I. Si certaines informations demandées ne sont pas immédiatement disponibles, dès lors qu'elles ne sont pas indispensables pour traiter rapidement l'incident, l'auteur du signalement peut transmettre les informations complémentaires dans un deuxième temps.

## 5. Analyses de l'incident de confidentialité

La RPRP détermine si l'on est bien en présence d'un incident de confidentialité en utilisant et complétant l'outil d'aide à la décision figurant à **l'ANNEXE III** .

Il s'agit de répondre successivement aux deux (2) questions suivantes :

5.1 Les informations qui font l'objet de l'incident sont-elles des renseignements personnels confidentiels ou non confidentiels ?

5.2 Ces renseignements personnels ont-ils fait l'objet :

- D'une consultation par une personne non autorisée à en prendre connaissance
- D'une transmission à une personne/entité non autorisée à les recevoir
- D'une utilisation à des fins non autorisées par la Loi ou par le titulaire de ces renseignements
- D'une perte ou d'un vol

**Dans l'affirmative :** Si les réponses aux deux (2) questions sont affirmatives, l'analyse se poursuit.

**Dans la négative :** Si l'une des réponses aux questions est négative, nous ne sommes pas en présence d'un incident de confidentialité, mais probablement en présence d'un incident de sécurité et aucune action particulière ne sera prise.

## 6. Évaluation de la situation

Le RPRP doit évaluer le risque qu'un préjudice soit causé à une personne concernée dont un RP est touché par l'incident de confidentialité.

Afin d'évaluer le risque de préjudice, le RPPR devra notamment répondre aux questions suivantes :

- **Quand l'incident a-t-il eu lieu?**
  - Fournir la date la plus précise de l'incident

- **Quand l'incident a-t-il été constaté?**
  - À quel moment l'incident a été constaté

- **Où l'incident a-t-il eu lieu?**
  - Dans les locaux de la Municipalité? Lesquels?
  - Chez un tiers détenant des renseignements personnels pour la Municipalité?
  - Est-ce un incident de confidentialité impliquant un lieu physique, un système informatique ou technologique, etc. ?
- **Quelles sont les causes probables de l'incident ?**
  - S'agit-il d'enjeux de sécurité physique, humaine, technologique, etc.?
  - Quelles mesures de sécurité étaient en place?
  - Pourquoi n'ont-elles pas été efficaces?
- **Qui peut avoir eu accès aux RP (employé non autorisé, mandataire, fournisseur, etc.)?**
  - Qui sont les personnes concernées (employés, fournisseur, citoyens, clients, etc.)?
  - Combien y a-t-il de personnes concernées?
  - Quelle est la nature des RP visés par l'incident (à caractère public, renseignements nominatifs, etc.)?
  - Il y a-t-il un risque de préjudice sérieux pour les personnes concernées?

## 7. Mise en place de mesure pour diminuer les risques

En fonction de l'évaluation de la situation, le RPRP doit s'assurer que des mesures raisonnables soient mises en place afin de diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se produisent.

Pour évaluer le risque de préjudice, il faut considérer notamment :

- La sensibilité des renseignements personnels en cause
- Les utilisations malveillantes possibles
- Les conséquences appréhendées de son utilisation
- La probabilité qu'il soit utilisé à des fins préjudiciables

## 8. Avis en cas de risque de préjudice sérieux

Lorsque l'évaluation de la situation mène à la conclusion qu'il y a un risque de préjudice sérieux pour les personnes concernées :

### 8.1 Avis à la CAI

Un avis doit être transmis avec diligence à la commission d'accès à l'information (CAI).

Un modèle du formulaire est disponible sur le site internet de la CAI , dont une copie figure à l'ANNEXE IV.

### 8.2 Avis à toutes les personnes concernées

la *Loi sur l'accès* n'exige pas que l'avis soit donné par écrit, il pourrait tout de même être donné par courrier, par courriel dans les meilleurs délais, aux personnes concernées de l'incident, et ce, conformément au modèle joint en Annexe A de la présente procédure. Dans le but d'agir rapidement et de diminuer ou d'atténuer les risques de préjudices sérieux, un avis public peut également être fait. Toutefois, la publication

d'un avis public n'exempte pas la Municipalité de l'envoi d'un avis à chaque personne concernée sauf dans les cas suivants :

- La transmission de l'avis peut causer un plus grand préjudice à la personne concernée;
- La transmission de l'avis représente une difficulté excessive pour la Municipalité;
- La Municipalité n'a pas les coordonnées de la personne concernée.
- Avant de communiquer avec la personne concernée, le RPRP doit s'assurer qu'il détient les bonnes coordonnées.

NOTE : La personne concernée n'a pas à être avisée tant que cela est susceptible d'entraver une enquête faite par une personne ou un organisme chargé par la loi de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

## 9. Inscrire l'information pertinente au registre des incident de confidentialité de la Municipalité

Le RPRP doit veiller à ce qu'un registre des incidents de confidentialité soit mis en place à la Municipalité.

Il doit également y inscrire tous les incidents de confidentialité, et ce, même s'ils ne présentent pas de risque de préjudice sérieux.

Les renseignements du registre doivent être conservés pour une période minimale de cinq (5) ans, après la date ou la période de prise de connaissance de l'incident par la Municipalité.

## 10. Mise à jour et modification de la procédure

La présente procédure devra être modifiée en fonction des changements législatifs, règlementaires, ou autres recommandations de la CAI ou du gouvernement, le cas échéant, afin de s'assurer qu'elle demeure en tout temps en conformité avec les lois applicables et les meilleures pratiques en cette matière.

En cas de modification, tous les employés de la Municipalité devront en être informés afin qu'ils puissent en prendre connaissance.

## 11. Entrée en vigueur

La présente politique prend effet à compter de son adoption.

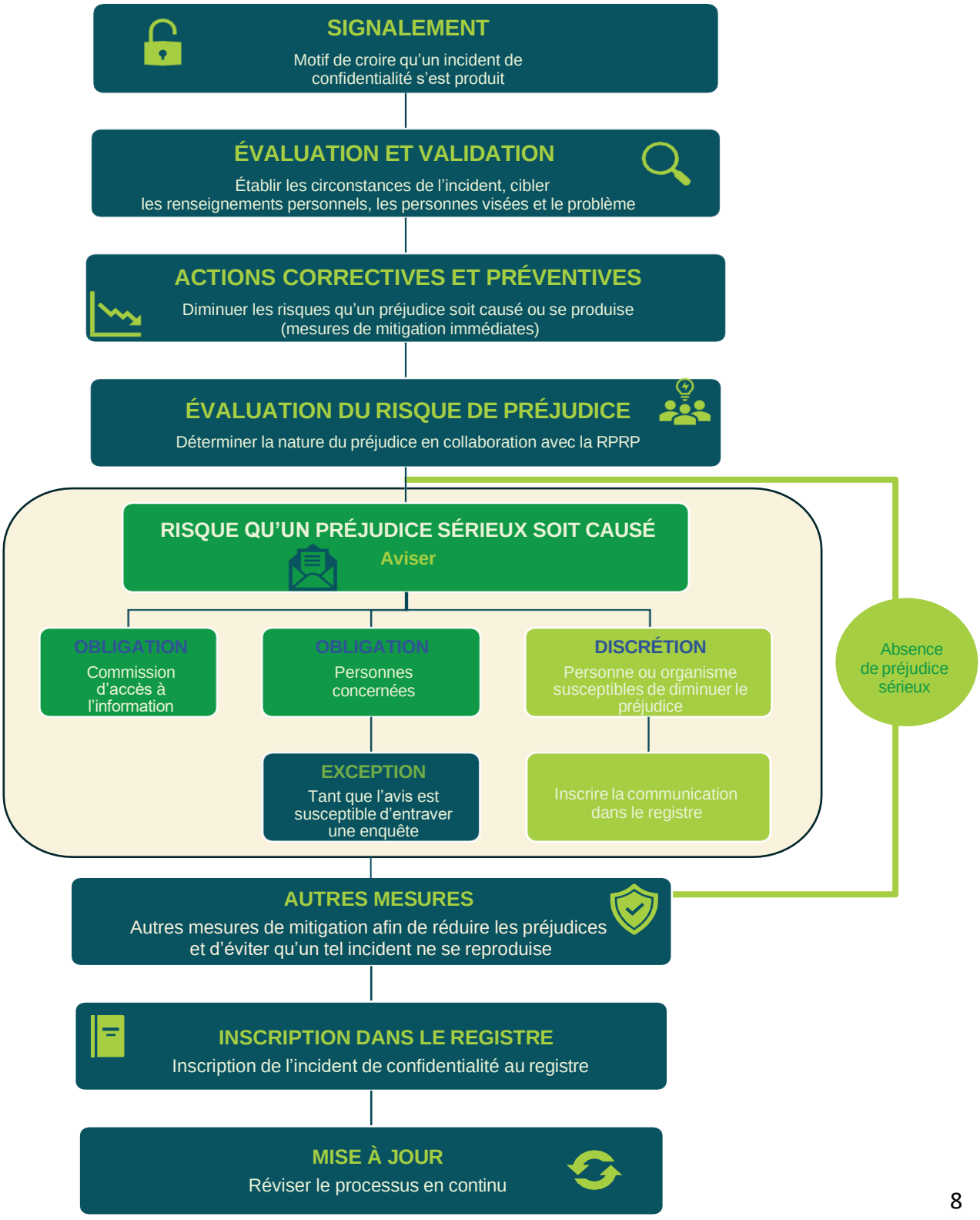
Jean-Guy Beaudet, maire

Josée Croteau, directrice-générale et greffière-trésorière

**Adoption de la politique** : 19 septembre 2023
Résolution n° 6467, 09-2023

**ANNEXE I**

Schéma de traitement d'un incident de confidentialité impliquant un renseignement personnel



**ANNEXE II**

Registre des incidents de confidentialité

## SOMMAIRE DE L'ÉVÉNEMENT

| | |
|---|---|
| Direction et division concernées par l'incident : | Nom et coordonnées de(s) l'employé(s) impliqué(s) lors de l'incident et nom de son gestionnaire (pour fins de cueillette d'informations) : |
| | |
| Description de l'incident (contexte, cause, source) : | |
| | |
| Date approximative et lieu de l'incident : | Date à laquelle l'incident a été porté à la connaissance d'un employé et la façon dont il a été connu : |
| Date de l'incident :<br><br>Lieu de l'incident : | |
| Type de personnes concernés par les renseignements personnels visés lors de l'incident (ex. : employés, citoyens, etc.) et le nombre de personnes visées : | |
| Type de personne concernées :<br><br>Nombre de personnes visées : | |
| Description des renseignements personnels visés par l'incident : | |
| | |

| |
|---|
| Sur quel support se trouvaient les renseignements personnels ? |
| |
| Est-ce que des mesures ont été prises immédiatement après la connaissance de l'incident ? |
| |
| Si concerne un incident technologique, est-ce que la Direction des TI en a été informée ? |
| |
| Est-ce que l'événement a été signalé ou sera signalé aux autorités policières (ex. : rapport de vol) ? Veuillez nous indiquer le numéro de référence, s'il y a lieu : |
| |
| Est-ce que l'incident concerne des renseignements personnels détenus par un fournisseur de service ? Si oui, lequel et identifiez une personne ressource chez ce fournisseur : |
| |

**Envoyez à l'adresse suivante :**

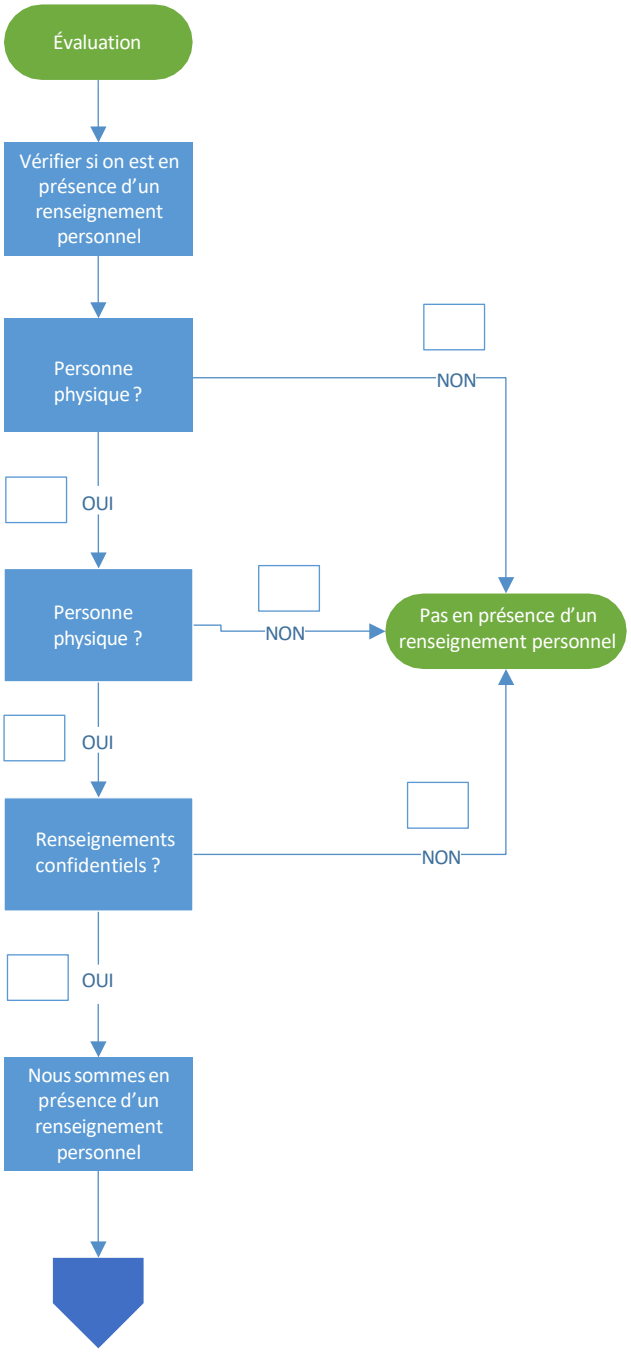
municipalite@ste-sophie-de-levrard.com

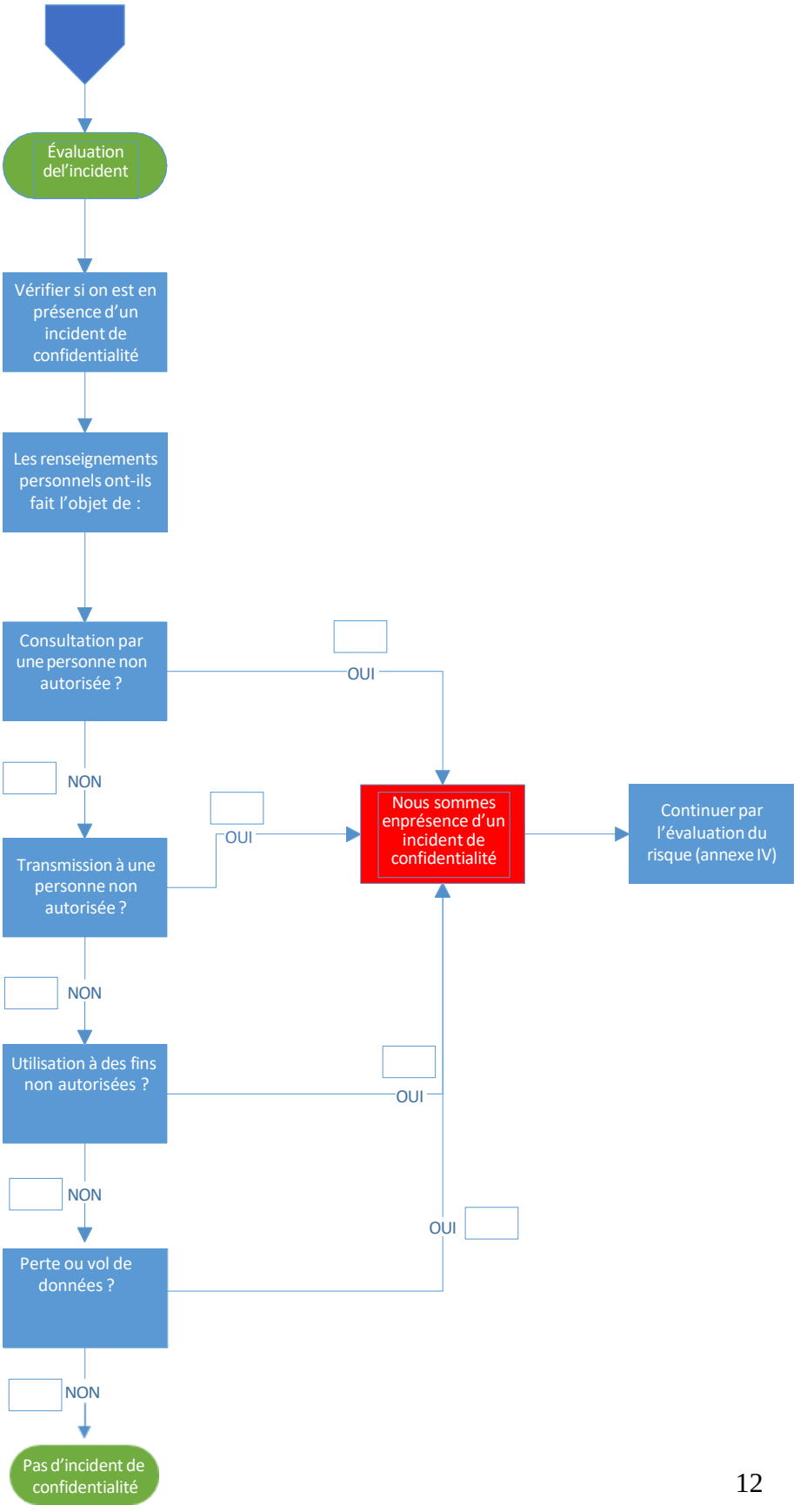
En cas d'urgence ou pour information,
veuillez communiquer avec la directrice générale et greffière-trésorière.

***ANNEXE III***

Evaluation de l'incident

## À REMPLIR PAR LA RPRP




Évaluation del'incident
Vérifier si on est en présence d'un incident de confidentialité
Les renseignements personnels ont-ils fait l'objet de :
Consultation par une personne non autorisée ?
OUI
NON
Transmission à une personne non autorisée ?
OUI
Nous sommes enprésence d'un incident de confidentialité
Continuer par l'évaluation du risque (annexe IV)
NON
Utilisation à des fins non autorisées ?
OUI
NON
Perte ou vol de données ?
OUI
NON
Pas d'incident de confidentialité

**ANNEXE IV**

Évaluation du risque de préjudice

| NIVEAU DU PRÉJUDICE | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **1. Sensibilité des renseignements personnels (cocher chaque RP concerné ou ajouter au besoin) *** | | | | | | | | | |
| **Faible** | | | **Modéré** | | | **Élevé** | | | |
| **Prénom** | | **Adresse** | | **Curriculum vitae** | | **DDN** | | **NAS** | |
| Nom | | État matrimonial | | Numéro de téléphone | | Adresse IP | | Numéro de permis de conduire | |
| Origine ethnique | | Renseignements scolaires | | Courriel | | Revenus | | Numéro d'assurance maladie | |
| Âge | | | | Dossier disciplinaire | | Cause de décès | | Données biométriques | |
| Sexe | | | | | | | | Numéro de compte bancaire | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

* Le cumul de plusieurs renseignements personnels (RP) augmente le niveau de sensibilité par rapport à un RP seul

| Péjudice sérieux ? | | |
|---|---|---|
| **OUI** | | **NON** |
| | | |
| Passer à l'étape 2 | | Pas besoin de notifier |

## ÉVENTUALITÉ DE SURVENANCE DU PRÉJUDICE

**2. Quelles sont les conséquences appréhendées ou utilisations malveillantes possibles de ces renseignements ?**

| | |
|---|---|
| Vol ou usurpation d'identité ? | |
| Fraude ou perte financière ? | |
| Perte liée aux affaires ? | |
| Dommages moraux (atteinte à la réputation, humiliation, discrimination) ? | |
| Répercussions sur la santé physique ou psychologique (stress) ? | |
| Conséquences négatives sur dossier de crédit ? | |
| Perte d'emploi ou perte d'occasions d'emploi ? | |
| Autres : | |

**3. Quelle est la probabilité que ces renseignements soient utilisés à des fins préjudiciables ?**

| | |
|---|---|
| Nulle | |
| Faible | |
| Moyenne | |
| Élevée | |

| |
|---|
| Sur quel support se trouvaient les renseignements personnels ? |
| |
| Est-ce que des mesures ont été prises immédiatement après la connaissance de l'incident ? |
| |
| Si concerne un incident technologique, est-ce que la Direction des TI en a été informée ? |
| |
| Est-ce que l'événement a été signalé ou sera signalé aux autorités policières (ex. : rapport de vol) ? Veuillez nous indiquer le numéro de référence, s'il y a lieu : |
| |
| Est-ce que l'incident concerne des renseignements personnels détenus par un fournisseur de service ? Si oui, lequel et identifiez une personne ressource chez ce fournisseur : |
| |

**Envoyez à l'adresse suivante :**

municipalite@ste-sophie-de-levrard.com

En cas d'urgence ou pour information,
veuillez communiquer avec la directrice générale et greffière-trésorière.

**ANNEXE V**

Formulaire de déclaration à la Commission d'accès à l'information du Québec

Commission d'accès à l'information du Québec

**Section réservée à la Commission**
Numéro de référence : _____
Date de réception : ___ / ___ / _____

## AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

### CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS ET QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEUX

**Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels**
**Loi sur la protection des renseignements personnels dans le secteur privé**

**Objet du présent formulaire**

Ce formulaire vise à permettre aux organisations[1] d'aviser la Commission d'accès à l'information (la Commission) de tout incident de confidentialité impliquant un renseignement personnel qu'elles détiennent et présentant un risque de préjudice sérieux.

On entend par « incident de confidentialité » :

- 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.

Assurez-vous de ne pas transmettre de renseignements personnels permettant d'identifier une personne dans ce formulaire et dans tout autre document que vous transmettrez à la Commission.

Soyez avisé que les informations inscrites dans le présent formulaire sont soumises à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Ainsi, certains renseignements, dont le nom de votre organisation et le fait qu'un incident l'impliquant est survenu, pourraient être communiqués publiquement.

Si vous manquez d'espace dans l'un des champs, joignez une annexe présentant l'ensemble de votre réponse lorsque vous transmettez le formulaire à la Commission et inscrivez « Voir annexe » dans le champ concerné.

Vous pouvez transmettre le formulaire et les documents joints 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] On entend par « organisation » : organisme public, personne qui exploite une entreprise, ordre professionnel, parti politique, député indépendant ou candidat indépendant, syndicat, association, organisme à buts non lucratifs, travailleur autonome et pigiste.

Commission d'accès à l'information du Québec

**Obligations de l'organisation**

- ✓ Évaluer si un incident de confidentialité représente un risque qu'un préjudice sérieux[2] soit causé aux personnes concernées par l'incident de confidentialité;
- ✓ Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent. Le fait de déclarer un incident de confidentialité à la Commission ne dispense pas une organisation de cette obligation;
- ✓ Aviser toute personne dont un renseignement personnel a été compromis par un incident de confidentialité si cet incident présente un risque qu'un préjudice sérieux soit causé. En cas de défaut, la Commission pourrait ordonner de le faire;
- ✓ Aviser la Commission, avec diligence, d'un incident de confidentialité impliquant un renseignement personnel qu'elle détient lorsque l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées;
- ✓ Transmettre à la Commission, dans les meilleurs délais, tout renseignement complémentaire dont elle prend connaissance après lui avoir transmis le présent avis;
- ✓ Inscrire l'incident déclaré dans son registre des incidents de confidentialité et communiquer ce dernier à la Commission sur demande.

Vous pouvez obtenir plus de renseignements au sujet de vos obligations en matière d'incident de confidentialité impliquant des renseignements personnels sur notre site Web à l'adresse https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/

**Rôle de la Commission au regard des incidents de confidentialité**

- La Commission s'assure que l'organisation respecte ses obligations légales lors d'un incident de confidentialité et qu'elle met en place les mesures nécessaires pour éviter que de nouveaux incidents de même nature ne se produisent.
- La Commission n'accompagne pas l'organisation dans la gestion des incidents de confidentialité.
- La Commission ne procède pas à la validation des mesures prises par l'organisation pour diminuer les risques qu'un préjudice soit causé ou pour éviter que de nouveaux incidents de même nature se produisent.
- Le fait d'aviser la Commission d'un incident de confidentialité ne peut servir à établir la conformité des pratiques d'une organisation à l'égard de ses obligations légales.

[2] Le préjudice sérieux n'a pas à s'être matérialisé. Il peut seulement être susceptible de se produire.

Commission d'accès à l'information du Québec

## 1. Identification de l'organisation concernée par l'incident de confidentialité
(Veuillez remplir la section A pour un organisme public et la section B pour une entreprise)

### A. Identification de l'organisme public

| | |
|---|---|
| Nom : | |
| Adresse : | |
| **Personne à contacter relativement à l'incident** | |
| Nom : | Fonction : |
| Téléphone : | Courriel : |
| **Personne responsable de la protection des renseignements personnels** ☐ **Même que précédent** | |
| Nom : | Fonction : |
| Téléphone : | Courriel : |

### B. Identification de l'entreprise

| | |
|---|---|
| Nom : | |
| Adresse du siège social : | |
| Numéro d'entreprise au Québec (selon le Registraire du Québec) : | |
| **Dirigeant principal** | |
| Nom : | Titre / fonction : |
| Téléphone : | Courriel : |
| **Personne à contacter relativement à l'incident** ☐ **Même que précédent** | |
| Nom : | Fonction : |
| Téléphone : | Courriel : |
| **Personne responsable de la protection des renseignements personnels** ☐ **Même que précédent** | |
| Nom : | Fonction : |
| Téléphone : | Courriel : |

Commission d'accès à l'information du Québec

## 2. Date et période de l'incident de confidentialité

| | |
|---|---|
| Date de l'incident : | Date de découverte de l'incident : |
| L'incident a eu lieu sur une période de : | |

## 3. Type d'incident de confidentialité

- ☐ Accès non autorisé par la loi à un renseignement personnel
- ☐ Utilisation non autorisée par la loi d'un renseignement personnel
- ☐ Communication non autorisée par la loi d'un renseignement personnel
- ☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

## 3.1 Causes et circonstances de l'incident de confidentialité

**Selon le type d'incident sélectionné ci-dessus, identifiez la ou les cause(s) de celui-ci :**

| | | | |
|---|---|---|---|
| ☐ Altération délibérée | ☐ Communication accidentelle | ☐ Communication délibérée sans autorisation | ☐ Consultation non autorisée |
| ☐ Cyberattaque (virus, logiciel espion, etc.) | ☐ Défaillance technique | ☐ Destruction accidentelle | ☐ Destruction volontaire sans autorisation |
| ☐ Divulgation accidentelle | ☐ Divulgation délibérée sans autorisation | ☐ Erreur humaine | ☐ Hameçonnage (phishing) |
| ☐ Ingénierie sociale | ☐ Perte d'accès aux renseignements | ☐ Perte de renseignements | ☐ Rançongiciel |
| ☐ Utilisation incompatible | ☐ Vol de renseignements | ☐ Autre<br>Précisez : | |

**Selon le type d'incident sélectionné ci-dessus, décrivez les circonstances de celui-ci :**

Commission d'accès à l'information du Québec

| Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident : | |
|---|---|
| ☐ Ordinateur de bureau | ☐ Dispositif amovible électronique |
| ☐ Papier | ☐ Clé USB |
| ☐ Serveur | ☐ CD |
| ☐ Bande sonore | ☐ Téléphone portable |
| ☐ Infonuagique (cloud) | ☐ Tablette |
| ☐ Vidéosurveillance | ☐ Ordinateur portable |
| ☐ Photo | ☐ Autre<br>Précisez : |

## 4. Description des renseignements personnels visés par l'incident de confidentialité

| | | |
|---|---|---|
| ☐ Nom<br>☐ Prénom | ☐ Adresse du domicile | ☐ Date de naissance ou<br>☐ Année ☐ Mois ☐ Jour ☐ Âge |
| ☐ Numéro de téléphone au domicile | ☐ Numéro du cellulaire | ☐ Adresse courriel personnelle |
| ☐ Numéro de permis de conduire | ☐ Numéro d'assurance sociale | |
| ☐ Numéro d'assurance maladie | ☐ Numéro de passeport | |
| ☐ Salaire | ☐ Fonction / occupation | |

☐ **Renseignements sur des employés**, clients ou bénéficiaires
Précisez :

☐ Renseignements médicaux
Précisez :

☐ Renseignements génétiques
Précisez :

☐ **Renseignements** scolaires / académiques
Précisez :

☐ **Renseignements** bancaires / numéro de compte / institution / placements / hypothèque
Précisez :

Commission d'accès à l'information du Québec

| | | | |
|---|---|---|---|
| ☐ Numéro de carte de crédit | ☐ Numéro d'identification personnel (NIP) | ☐ Nom du détenteur | ☐ Code de sécurité à trois chiffres |
| ☐ Numéro de carte de débit | ☐ Numéro d'identification personnel (NIP) | ☐ Nom du détenteur | |

☐ Autres renseignements personnels

Précisez :

☐ Impossible de fournir une description des renseignements personnels visés

Expliquez :

## 5. Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employés, de clients, d'étudiants, de patients, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens :

## 6. Évaluation par l'organisation du fait qu'un risque de préjudice sérieux puisse être causé aux personnes concernées par l'incident de confidentialité

Décrivez les éléments amenant l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées. Ce risque peut être attribuable au fait qu'il s'agisse de renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables. Dans ce cas, indiquez les conséquences appréhendées de leur utilisation sur les personnes concernées.

Commission d'accès à l'information du Québec

| Décrivez les raisons qui supportent l'**existence d'**un risque de préjudice sérieux **pour les** personnes concernées par l'incident. |
|---|
| |
| Le responsable de la protection des renseignements personnels de votre organisation a-t-il été consulté pour procéder à l'évaluation du risque de préjudice? |
| ◯ Oui ◯ Non |

## 7. Avis de l'organisation aux personnes concernées
**(Vous pouvez joindre une copie de l'avis transmis aux personnes concernées)**

**L'organisation a-t-elle avisé les personnes concernées par l'incident de confidentialité?**

◯ Non
◯ Oui. L'avis a été fait par :

| | | |
|---|---|---|
| ☐ Lettre transmise par courrier | ☐ Courriel | ☐ Message texte |
| ☐ Verbal (ex. par téléphone) | ☐ En personne | ☐ Autre<br>Précisez : |

Date de l'avis :

Si les personnes concernées n'ont pas encore été avisées, quelles mesures seront prises par l'organisation afin de le faire?

| | | |
|---|---|---|
| ☐ Lettre transmise par courrier | ☐ Courriel | ☐ Message texte |
| ☐ Verbal (ex. par téléphone) | ☐ En personne | ☐ Autre<br>Précisez : |

Date de l'avis prévu :

☐ Aucune notification de l'incident aux personnes concernées n'est prévue.
Expliquez :

Commission d'accès à l'information du Québec

## 7.1 Contenu de l'avis aux personnes concernées

**Sélectionnez les éléments contenus dans l'avis transmis aux personnes concernées par l'organisation.**

- ☐ Une description des renseignements personnels visés par l'incident
- ☐ Une brève description des circonstances de l'incident
- ☐ La date ou la période où l'incident a eu lieu
- ☐ Une brève description des mesures que l'organisation a prises ou entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé
- ☐ 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
- ☐ Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident

**Y a-t-il des personnes concernées par l'incident qui ne seront pas avisées par l'organisation?**

- ◯ Non.
- ◯ Oui. Combien :

  Expliquez :

## 7.2 Avis public aux personne concernées

**L'avis aux personnes concernées a-t-il été fait, exceptionnellement, au moyen d'un avis public?**

- ◯ Non
- ◯ Oui. Sélectionnez la raison applicable :

  - ☐ Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée.

    Expliquez :
  - ☐ Le fait de transmettre l'avis est susceptible présenter une difficulté excessive pour l'organisation.

    Expliquez :
  - ☐ L'organisation n'a pas les coordonnées des personnes concernées.

    Expliquez :

Commission d'accès à l'information du Québec

## 8. Obligation de diminuer le risque de préjudice

Quelles mesures ont été prise dès la découverte de l'incident, notamment afin de réduire les risques de préjudice aux personnes concernées?

Dans quel délai ces mesures ont-elles été prises?

Est-ce que des mesures ont été prises après la découverte de l'incident afin d'éviter que de nouveaux incidents de même nature se reproduisent?

- ◯ Non
- ◯ Oui. Précisez :

Y a-t-il des mesures prévues qui n'ont pas encore été prises?

- ◯ Non
- ◯ Oui. Précisez :

Indiquez la date de mise en place des mesures prévues :

*Une organisation doit transmettre à la Commission tout renseignement relatif à l'incident de confidentialité dont elle prend connaissance après lui avoir transmis le présent avis. L'information complémentaire doit alors être transmise dans les meilleurs délais à compter de cette connaissance.*

Est-ce que des informations supplémentaires seront transmises à la Commission concernant l'incident rapporté?

- ◯ Non
- ◯ Oui. Précisez lesquelles et indiquez l'échéancier prévu :

Commission d'accès à l'information du Québec

## 9. Signature

| | |
|---|---|
| Prénom : | Nom : |
| Fonction : | Lieu / Ville : |
| Date de transmission du formulaire à la Commission : | |
| Pour le compte de : ◯ l'organisme ◯ l'entreprise | |
| *Je déclare que les renseignements concernant l'incident de confidentialité fournis dans la présente déclaration sont complets et conformes aux faits.* | |
| Signature : | |