PROCÉDURE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL

TABLE DES MATIERES

PRÉAMBULE

La Municipalité de Ferme-Neuve (l'« **Organisme municipal** ») est responsable de la protection des renseignements personnels qu'elle détient, que leur conservation soit assurée à l'interne ou par un tiers. Les renseignements personnels sont confidentiels, sauf dans la mesure prévue par la législation. Toute personne qui, dans le cadre de ses fonctions, a accès à un renseignement personnel détenu par l'Organisme municipal doit prendre les moyens nécessaires pour en assurer la protection et la confidentialité. Néanmoins, des incidents de confidentialité impliquant un renseignement personnel détenu par l'Organisme municipal peuvent survenir, et c'est pourquoi l'Organisme municipal a choisi de se doter de la présente Procédure de gestion des incidents de confidentialité impliquant un renseignement personnel.

La présente procédure met en place un cadre de gestion des incidents de confidentialité conforme aux obligations en matière de protection des renseignements personnels suivant l'adoption de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*.

1. OBJECTIF ET CADRE NORMATIF

La présente procédure a pour but de gérer les incidents de confidentialité et limiter leurs éventuelles conséquences négatives pour les Personnes concernées et l'Organisme municipal. Elle établit la démarche à suivre en cas d'incident de confidentialité impliquant un renseignement personnel détenu par l'Organisme municipal, précise les rôles et les responsabilités des intervenants en cas d'incident, détermine les modalités de la tenue d'un registre des incidents et rappelle l'obligation d'effectuer les déclarations obligatoires requises en cas d'incident de confidentialité impliquant un renseignement personnel.

Le cadre normatif de cette procédure comprend principalement :

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 modifiée par la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, RLRQ, c. 25 (la « **Loi sur l'accès** »);
- Règlement sur les incidents de confidentialité, C A-2.1, r. 3.1 ;
- Politique de sécurité de l'information ;
- Politique de confidentialité.

2. CHAMP D'APPLICATION

La présente procédure s'applique à tous les employés de l'Organisme municipal et à tous les tiers auxquels l'Organisme municipal communique des renseignements personnels, y compris tous fournisseurs ou partenaires, incluant les sous-traitants (ci-après un « **Tiers** ») ayant connaissance d'un incident de confidentialité en lien avec les renseignements personnels communiqués.

3. DÉFINITIONS

Dans le cadre de la présente procédure, les termes ci-après ont les définitions suivantes. Ils peuvent être complétées par toute autre politique, directive ou procédure y faisant référence.

- **Commission :** Commission d'accès à l'information du Québec;

- **Incident de confidentialité** : tout accès, utilisation, communication d'un renseignement personnel non autorisé par la loi, de même que sa perte ou toute autre forme d'atteinte à sa protection.

En voici quelques exemples :

- Un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions;

- Un pirate informatique s'infiltre dans un système;

- Une personne utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;

- Une communication est effectuée par erreur à la mauvaise personne, contenant des renseignements personnels;

- Une personne perd ou se fait voler des documents contenant des renseignements personnels;

- Une personne s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

Personne concernée : personne physique dont les Renseignements personnels sont exposés à un risque en raison de la survenance d'un Incident de confidentialité.

Renseignement personnel : tout renseignement 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. Pour davantage d'exemples de renseignement personnel, il faut se référer à la Politique cadre concernant la protection des renseignements personnels.

RPRP : désigne la personne physique qui veille à assurer le respect et la mise en œuvre des Lois applicables sur la protection de la vie privée au sein de l'Organisme municipal.

4. ÉQUIPE D'INTERVENTION EN CAS D'INCIDENT DE CONFIDENTIALITE

Dans le but de gérer les Incidents de confidentialité, l'Organisme municipal doit mettre en place une équipe d'intervention multidisciplinaire composée du RPRP et de personnes compétentes et qualifiées issues des différents départements comme les services informatiques, de la sécurité informatique, des affaires juridiques, des finances, des opérations et des relations avec le public. L'équipe peut être une équipe physique (locale) ou virtuelle (plusieurs emplacements) qui répond à tout Incident de confidentialité suspect ou présumé.

Le RPRP de l'Organisme municipal ou la personne désignée parmi les personnes compétentes agit comme chef de l'équipe d'intervention et il ou elle est responsable de nommer les membres de l'équipe en cas d'Incident de confidentialité. L'équipe doit être créée, qu'il y ait eu ou non une violation.

L'équipe doit s'assurer qu'il existe une préparation nécessaire à une intervention en cas de violation de Renseignements personnels, ainsi que les ressources et la préparation nécessaires (telles que les listes d'appels, la substitution de rôles clés, les exercices de bureau, ainsi que l'examen requis des politiques, procédures et pratiques de l'Organisme municipal). Pour s'assurer du niveau de préparation de l'équipe d'intervention, le RPRP devrait réaliser au moins un exercice de simulation par an.

La mission de l'équipe est de fournir une réponse immédiate, efficace et habile à toute violation de Renseignements personnels suspecté, présumé ou réel affectant l'Organisme municipal.

Si nécessaire, les membres de l'équipe peuvent également impliquer des parties externes (par exemple, un fournisseur de sécurité de l'information pour effectuer des tâches de criminalistique numérique ou une agence de communication externe pour aider l'Organisme municipal dans les besoins de communication de crise).

Le chef de l'équipe d'intervention, en cas d'incident de confidentialité, peut choisir d'ajouter du personnel supplémentaire à l'équipe dans le but de traiter une violation de Renseignements personnels spécifique. L'équipe d'intervention en cas d'Incident de confidentialité peut traiter plus d'une violation de Renseignements personnels suspecté, présumé ou réel à la fois. Bien que l'équipe de base puisse être la même pour chaque violation de Renseignement personnels, il n'y a aucune exigence pour cela.

L'équipe d'intervention, en cas d'Incident de confidentialité, doit être prête à répondre à une atteinte à la protection des Renseignements personnels suspecté, présumé ou réel 24 heures sur 24, 7 jours sur 7, toute l'année. Par conséquent, les coordonnées de chaque membre de l'équipe d'intervention en cas d'incident de confidentialité, y compris les coordonnées personnelles, seront stockées dans un emplacement central et seront utilisées pour constituer l'équipe chaque fois qu'une notification d'une violation de Renseignements personnels est reçue.

5. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Dès qu'une personne, employé ou tiers, a des motifs de croire que s'est produit un incident de confidentialité, elle doit signaler l'incident en complétant une déclaration d'incident de confidentialité.

5.1 Déclaration d'incident de confidentialité

Pour déclarer un bris de confidentialité en tant qu'employé de la municipalité, il convient de suivre les étapes suivantes :

1. **Identification du bris de confidentialité** : L'employé doit noter tous les détails pertinents du bris, y compris la nature de l'information divulguée, les personnes impliquées, la date et l'heure du bris, et comment le bris a été découvert.
2. **Documentation** : Il est important que l'employé documente le plus d'information possible concernant le bris. Cela inclut des copies de toute communication pertinente, des preuves tangibles du bris, et toute autre information qui pourrait être utile pour l'enquête.
3. **Notification immédiate** : L'employé doit informer immédiatement le RPRP. Cela peut se faire par écrit ou par une conversation directe, mais un suivi écrit est recommandé pour des raisons de traçabilité.

- **Courriel/Formulaire** : Le formulaire doit être adressé au RPRP. Voici un exemple de déclaration que l'employé pourrait envoyer :

Objet : Déclaration de bris de confidentialité

Bonjour [Nom du RPRP],

Je vous écris pour vous informer d'un bris de confidentialité que j'ai découvert le [date] à [heure]. Voici les détails de l'incident :

- Nature de l'information divulguée : [description]
- Personnes impliquées : [noms]
- Comment le bris a été découvert : [description]

J'ai joint à ce courriel toute la documentation pertinente.

Je reste disponible pour fournir toute information supplémentaire ou pour discuter de l'incident en détail.

Cordialement,

[Votre nom]
[Votre poste]

4. **Suivi** : L'employé doit effectuer un suivi avec le RPRP pour vérifier que la déclaration a bien été reçue et qu'une enquête est en cours. Il doit offrir sa coopération pour toute étape supplémentaire de l'enquête.
5. **Confidentialité** : Pendant tout ce processus, l'employé doit maintenir la confidentialité de l'incident et des personnes impliquées, en partageant l'information uniquement avec ceux qui ont besoin de savoir.

Pour les tiers, un lien vers la déclaration est disponible sur le site Web de l'Organisme municipal.

5.2 Avis au gestionnaire

En plus de compléter la déclaration d'incident, les employés doivent également aviser leur gestionnaire sans délai.

L'employé, sa ou les direction(s) impliquées de même que tout tiers signalant l'incident doivent collaborer à l'analyse de l'incident.

La déclaration de l'incident est reçue par le RPRP de même que par le directeur des technologies de l'information.

6. DÉTECTION ET ÉVALUATION PRÉLIMINAIRE

Le RPRP prend connaissance de la déclaration d'incident et effectue une évaluation préliminaire de la situation. S'il détermine que cette dernière correspond à un incident de confidentialité, il transmet son évaluation préliminaire et la déclaration d'incident au RPRP. Il est important de noter la différence entre un incident de sécurité et un incident de confidentialité. À cet effet, un incident de sécurité peut n'entrainer aucune compromission de renseignements personnels, et de ce fait, ne constitue pas un incident de confidentialité. Un schéma des facteurs déterminants à observer se retrouver à l'Annexe 1 de la présente Procédure.

7. ÉVALUATION DU RISQUE ET MESURES À PRENDRE

Sur réception de la déclaration d'incident et de l'évaluation préliminaire du RPRP, celui-ci :

a. Évalue le risque qu'un préjudice sérieux soit causé à une personne;

b. S'assure que les mesures préventives et correctrices raisonnables existantes sont adéquates pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Dans le cas contraire, le RPRP détermine les mesures devant être prises pour les corriger.

Le RPRP doit intervenir aussi souvent que requis, selon la gravité de l'incident. Il peut convoquer tout membre du personnel jugé utile et doit documenter ses travaux, en répondant aux questions prévues à l'Annexe 2. En fonction de la gravité de l'Incident de confidentialité, le RPRP peut également impliquer des parties externes tels qu'un fournisseur de sécurité de l'information pour effectuer des enquêtes criminalistiques numériques ou une agence de communication externe pour aider l'Organisme municipal lors de communications en situation de crise, etc.

L'évaluation du risque qu'un préjudice sérieux soit causé à une personne doit être établie en application de la méthodologie d'évaluation de risque décrite dans le document intitulé : « **Analyse de risque de préjudice sérieux pour une personne concernée** » et en répondant aux questions prévues à l'Annexe 1.

Elle doit prendre en compte la sensibilité du Renseignement personnel, les conséquences appréhendées et la probabilité de son utilisation à des fins préjudiciables.

8. MESURES URGENTES POUR LIMITER L'ATTEINTE À LA VIE PRIVÉE

En cas d'incident de confidentialité, la ou les directions impliquées, de même que la direction des technologies de l'information, au besoin, doivent prendre toute mesure urgente requise pour limiter les conséquences pour les personnes concernées, notamment la possibilité d'utilisation malveillante des renseignements personnels, l'usurpation ou le vol d'identité.

9. DÉCLARATION DE L'INCIDENT

Si l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées par les renseignements personnels, le RPRP doit, avec diligence, transmettre un avis à la Commission et aux personnes concernées par les renseignements personnels, si nécessaire. Le contenu de ces avis doit être conforme au *Règlement sur les incidents de confidentialité*, tel que détaillé à l'Annexe 3 des présentes.
Le RPRP doit également aviser la Personne concernée de l'incident, s'il existe un risque probable de préjudice sérieux. Cet avis, qui doit être transmis sans délai, doit être rédigé dans un langage clair et simple et contenir les informations exigées suivant les dispositions du Règlement sur les incidents de confidentialité, telles que détaillées à l'Annexe 3 des présentes.

Lorsque l'incident de confidentialité constitue ou peut être qualifié de criminel, le RPRP doit aviser les services de police compétents.

Le RPRP peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.
Finalement, le RPRP avise, avec diligence, la personne responsable des contacts avec les assureurs, le cas échéant.

10. ÉVALUATION APPROFONDIE DE LA SITUATION ET PRÉVENTION

Le RPRP doivent effectuer une évaluation approfondie de l'incident afin d'éviter que de nouveaux incidents de même nature ne se produisent. Cette évaluation approfondie doit être documentée et contenir notamment les informations prévues à l'Annexe 4.

L'évaluation approfondie doit être transmise sur demande au plus haut dirigeant de l'Organisme municipal lorsque celle-ci est complétée. Le plus haut dirigeant de l'Organisme municipal peut également la transmettre au conseil municipal de l'Organisme s'il juge pertinent de le faire.

11. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

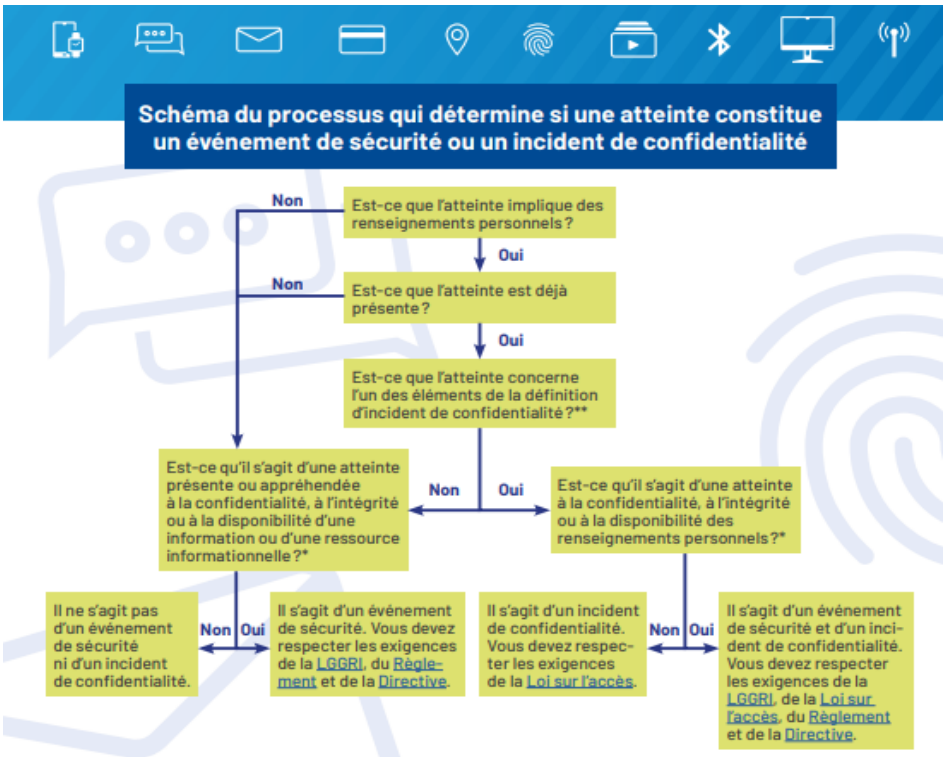
Le RPRP doit tenir un registre des incidents de confidentialité conforme au *Règlement sur les incidents de confidentialité*. Le RPRP doit y consigner tout incident de confidentialité indifféremment de sa gravité et de l'existence ou non de risque de préjudice sérieux. Une copie du registre doit être transmise à la Commission sur demande.

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'Organisme municipal a pris connaissance de l'incident.

12. RESPONSABLE DE LA PROCÉDURE

Le RPRP est responsable de l'application de la présente procédure.

ANNEXE 1 : INCIDENT DE SÉCURITÉ ET INCIDENT DE CONFIDENTIALITÉ



ÉVÉNEMENT DE SÉCURITÉ*

Définition (paragraphe 7 de l'article 2 de la Directive et paragraphe 1 de l'article 1 du Règlement) :

Toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'un organisme public.

Comparaison avec un incident de confidentialité :

Dans la grande majorité des cas, un incident de confidentialité est également un événement de sécurité. Une communication ou un accès non autorisé par la Loi ainsi que la perte d'un renseignement personnel constituent, dans tous les cas, des événements de sécurité.

Pour l'utilisation non autorisée par la loi d'un renseignement personnel et pour les autres atteintes à la protection d'un tel renseignement, chaque situation doit être évaluée séparément.

INCIDENT DE CONFIDENTIALITÉ**

Définition (article 63.9 de la Loi sur l'accès) :

On entend par « incident de confidentialité » :

1- l'accès non autorisé par la loi à un renseignement personnel ;

2- l'utilisation non autorisée par la loi d'un renseignement personnel ;

3- la communication non autorisée par la loi d'un renseignement personnel ;

4- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Comparaison avec un événement de sécurité :

Les événements de sécurité couvrent l'atteinte à une information ou à une ressource informationnelle alors que l'incident de confidentialité ne concerne que l'atteinte à un renseignement personnel. Les atteintes couvertes par un événement de sécurité peuvent être présentes ou appréhendées, alors que celles qui constituent un incident de confidentialité doivent être présentes. Un incident de confidentialité couvre principalement une seule forme d'atteinte : la confidentialité. Cependant, dans certains cas, il peut s'accompagner d'une atteinte à la disponibilité ou à l'intégrité.

Votre gouvernement

Québec

ANNEXE 2 : ÉVALUATION DU RISQUE ET MESURES À PRENDRE

1. Nécessité d'évaluer le risque de préjudice sérieux ou risque réel de préjudice grave

Pour tout Incident de confidentialité, l'Organisme municipal doit évaluer la gravité du risque de préjudice qui peut être causé aux personnes concernées visées par l'Incident de confidentialité. Pour ce faire, elle doit considérer, notamment :

1. La sensibilité des renseignements concernés;
2. Les conséquences appréhendées de leur utilisation;
3. La probabilité qu'ils soient utilisés à des fins préjudiciables.

L'Organisme municipal doit consulter son RPRP. Elle peut également impliquer d'autres acteurs, comme le responsable de la sécurité de l'information ou des experts externes. Si l'analyse fait ressortir un risque de préjudice sérieux ou risque réel de préjudice grave, l'Organisme municipal doit aviser l'Autorité de contrôle et les personnes concernées de l'Incident de confidentialité.

Dans le cas contraire, elle doit tout de même poursuivre ses efforts pour réduire les risques et éviter qu'un incident de même nature ne se reproduise.

2. Méthodologie d'évaluation de risque

Le risque de préjudice sérieux ou risque réel de préjudice grave peut être calculé à l'aide de la méthodologie suivante.

ÉTAPE 1

Contexte de traitement des données **(CTD)** : Dans cette composante, le type de renseignements personnels et la nature des activités de traitement sont classés et notés.

Tableau préliminaire du résultat de base:

Type	Description	Résultat de base
Simple	Ex. : données biographiques, coordonnées, nom complet, données sur l'éducation, la vie de famille, l'expérience professionnelle, etc.	1
Comportemental	Ex. : emplacement, données de trafic, données sur les préférences et les habitudes personnelles, etc.	2
Financière	Tout type de données financières (ex.: revenus, transactions financières, relevés bancaires, placements, cartes de crédit, factures, etc.), comprend des données relatives aux bénéfices sociaux liées à l'information financière	3
Sensible	Tout type de données sensibles (ex. : santé, affiliation politique, vie sexuelle, orientation religieuse)	4

Facteurs faisant augmenter le résultat de base:

Type	Description	Résultat
Simple	Lorsque le volume de « données simples » et/ou les caractéristiques du responsable du traitement sont tels que certains profils de la personne peuvent être déduites ou que des hypothèses sur la situation sociale ou financière de la personne peuvent être formulées.	2
Simple	Lorsque le volume de « données simples » et / ou les caractéristiques du responsable du traitement peuvent conduire à des hypothèses sur le statut de santé de l'individu, ses préférences sexuelles, ses croyances politiques ou religieuses.	3
Simple	Lorsque les données correspondent à certaines caractéristiques de la personne (ex.: groupes vulnérables, mineurs), l'information peut être essentielle à sa sécurité personnelle ou à son état physique ou psychologique.	4
Comportemental	Lorsque le volume de « données comportementales » et/ou les caractéristiques du responsable du traitement sont tels qu'un profil de l'individu peut être créé, exposant ainsi des informations détaillées sur sa vie quotidienne et ses habitudes.	3
Comportemental	En raison de la nature et/ou du volume de l'ensemble des données spécifiques, des informations financières complètes (ex. : carte de crédit, relevé bancaire, rapport de crédit, état financier) sont divulguées de manière à permettre que de la fraude ou un profil social ou financier détaillé soit créé à l'égard de la personnes concernée.	4
Financière	En raison de la nature et/ou du volume de l'ensemble des données spécifique, des informations financières complètes (ex. : carte de crédit, relevé bancaire, rapport de crédit, état financier) sont divulguées de manière à permettre que de la fraude ou un profil social ou financier détaillé soit créé à l'égard de la personnes concernée.	4

Facteurs faisant diminuer le résultat de base:		
Type	**Description**	**Résultat**
Comportemental	Lorsque la nature de l'ensemble des données ne fournit pas de renseignements substantiels sur les informations liées au comportement de la personne ou que les données peuvent être recueillies facilement (indépendamment de l'incident) par l'entremise de sources accessibles au public (ex.: combinaison d'informations provenant de services Web).	1
Financière	Lorsque la nature de l'ensemble des données ne fournit aucun aperçu substantiel des renseignements financiers de la personne (ex.: le fait qu'une personne est le client d'une certaine banque sans plus de détails).	1
Financière	Lorsque l'ensemble des données spécifiques comprend certains renseignements financiers, mais ne fournit toujours pas d'informations significatives sur la situation financière de la personne (ex. : simples numéros de compte bancaire sans plus de détails).	2
Sensitive	Lorsque la nature de l'ensemble de données ne fournit aucun aperçu substantiel de l'information comportementale de la personne ou que les données peuvent être recueillies facilement (indépendamment de l'atteinte) par l'entremise de sources accessibles au public (p. ex., une combinaison de renseignements provenant de recherches sur le Web).	1
Sensitive	Lorsque la nature des données peut conduire à des hypothèses générales.	2
Sensitive	Lorsque la nature des données peut mener à des hypothèses sur les renseignements de nature délicate.	3

Méthode de calcul de la première étape :

1) Sélectionner le score de 1 à 4 dans le tableau des « résultat de base »;
2) (si applicable) Augmenter le score obtenu à (1) par le pointage de 2 à 4 selon le tableau « augmenter le résultat de base »;
3) (si applicable) Réduire le score obtenu à (1) ou (2 – seulement si applicable) par le pointage de 1 à 3 selon le tableau « réduire le résultat de base ».

Le score final se situe à pas plus de 4 et pas moins de 1.

ÉTAPE 2

Facilité dans laquelle la personne concernée peut être identifiée **(FI)** : Lors du calcul du résultat, vous devez tenir compte à la fois de l'identification directe d'une seule personne concernée unique à partir des

données compromises et de l'identification indirecte d'une personne concernée en combinant les données compromises avec d'autres sources.

Niveau	Description	Résultat
Négligable	Il est extrêmement difficile de faire correspondre les données à une personne en particulier, mais cela pourrait quand même être possible dans certaines conditions.	0,25
Limité	Il est possible mais difficile de faire correspondre les données à une personne en particulier ayant accès à des sources de données supplémentaires.	0,50
Significatif	L'identification est possible inderectement à partir des données faisant l'objet de l'incident avec une simple recherche de base permettant de découvrir l'identité de l'individu.	0,75
Maximum	L'identification est possible directement à partir des données faisant l'objet de l'incident sans nécessiter de recherche spéciale pour découvrir l'identité de la personne.	1,00

Méthode de calcul de la deuxième étape :
Attribuer une cote selon le niveau de facilité d'identification directe ou indirecte de la personne concernée selon le tableau précédent.

ÉTAPE 3

Circonstances de l'incident **(CI)** : les circonstances de l'incident, contrairement aux deux premières composantes (CTD et FI) qui examinent uniquement la nature inhérente des données, évaluent ce qui s'est réellement passé pendant l'incident. La notation est basée sur la nature de la perte de confidentialité, d'intégrité et de disponibilité. De plus, le résultat final sera influencé lorsque l'incident est considéré comme non intentionnel ou qu'il résulte d'une intention malveillante (i.e. l'acte était délibéré et non accidentel).

Niveau	Description	Résultat
Confidentialité	Compromis à un certain nombre de destinataires connus (ex., les dossiers d'un client envoyés à un autre client non lié).	0,25
Confidentialité	Compromis à un nombre inconnu de destinataires inconnus (ex. : un site web mal configuré rend les données accessibles au public sur Internet).	0,50
Integrité	Données modifiées et éventuellement utilisées de manière incorrecte ou illégale, mais avec la possibilité de récupérer.	0,25
Intégrité	Données modifiées et éventuellement utilisées de manière incorrecte ou illégale, mais avec l'impossibilité de récupérer.	0,50
Disponibilité	Non disponible pendant un temps défini.	0,25
Disponibilté	Les données ne peuvent être récupérées du l'entreprise ou des personnes concernées.	0,50
Malicieux	La violation était due à une action intentionnelle visant à nuire à l'entreprise ou aux personnes concernées (ex.: attaque ransomeware).	0,50

Méthode de calcul de la troisième étape :
Attribuer une cote selon la nature de la perte de confidentialité, d'intégrité et de disponibilité selon le tableau précédent.

ÉTAPE 4
Calcul de l'indice de sévérité de l'Incident de confidentialité

Méthode de calcul de la quatrième étape :

$$\text{Sévérité} = (\text{CTD} \times \text{FI}) + \text{CI}$$

Les indices CTD, FI et CI se trouvent aux étapes précédentes.
Selon le chiffre obtenu (1 à 4,5), la classification du risque de préjudice sérieux ou risque réel de préjudice grave se fait selon le tableau suivant :

Résultat de sévérité	Description	Classification
Sévérité 2	Les individus ne seront pas affectés ou peuvent rencontrer quelques inconvénients, qu'ils surmonteront sans aucun problème (temps passé à saisir à nouveau des informations, des désagréments, des irritations dues à l'incident, etc.).	BAS
Sévérité 2 3	Les individus peuvent rencontrer des inconvénients importants qu'ils seront en mesure de surmonter malgré quelques difficultés (coûts supplémentaires, refus d'accès aux services de l'entreprise, peur, manque de compréhension, stress, malaises physiques mineures, etc.).	MÉDIUM
Sévérité 3 4	Les individus peuvent faire face à des conséquences importantes, qu'ils devraient être en mesure de surmonter, mais avec de graves difficultés (détournement de fonds, mise sur liste noire par les banques, dommages matériels, perte d'emploi, citation à comparaître, détérioration de la santé, etc.).	HAUT
Sévérité 4	Les individus peuvent faire face à des conséquences importantes, voire irréversibles, qu'ils peuvent ne pas surmonter (difficultés financières telles qu'une dette substantielle ou l'incapacité de travailler, les maladies psychologiques ou physiques à long terme, le décès, etc.).	TRÈS HAUT

ANNEXE 3 : CONTENU DES AVIS

Conformément au Règlement sur les incidents de confidentialité :

1. Avis aux personnes concernées

L'avis aux personnes concernées doit contenir les renseignements suivants :

a. 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 ;

b. Une brève description des circonstances de l'incident;

c. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de la période ;

d. 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 ;

e. 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;

f. Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

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

a. Lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la Personne concernée ;

b. Lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'Organisme municipal ;

c. Lorsque l'Organisme municipal n'a pas les coordonnées de la personne concernée.

Quand un Incident de confidentialité présente le risque d'un préjudice sérieux, l'Organisme municipal doit aviser par écrit les personnes concernées.

L'avis aux personnes concernées doit contenir les informations suivantes :

SECTION III
AVIS AUX PERSONNES CONCERNÉES

5. L'avis à la personne dont un renseignement personnel est concerné par un incident qui présente un risque qu'un préjudice sérieux soit causé, donné en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), 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 la survenance 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.

6. L'avis visé à l'article 5 est transmis à la personne concernée par l'incident de confidentialité.
Malgré le premier alinéa, l'avis visé à l'article 5 est 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 accrut 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, afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice, l'avis visé à l'article 5 peut également être donné au moyen d'un avis public. Dans ce cas, l'organisation demeure toutefois tenue de transmettre, avec diligence, un avis à la personne concernée, à moins que l'une des circonstances énoncées au deuxième alinéa ne s'applique à sa situation.
En application du présent article, un avis public peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée.

Lors de l'envoi de l'avis aux personnes concernées dont un renseignement personnel est concerné par un incident de confidentialité qui présente un risque qu'un préjudice sérieux soit causé, l'Organisme municipal peut consulter et remplir le formulaire des *Éléments devant paraître dans un avis destiné à une personne dont un renseignement personnel est concerné par un incident de confidentialité qui présente un risque qu'un préjudice sérieux soit causé* (https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/incidents-confidentialite/liste-verification-incident-confidentialite-prp.pdf).

2. Avis à la Commission d'accès à l'information (CAI)

Lorsque la violation de Renseignements personnels ou la violation présumée de Renseignements personnels affecte des Renseignements personnels traités par l'Organisme municipal, les actions suivantes sont effectuées par le Responsable de la protection des renseignements personnels :

1. L'Organisme municipal doit établir si la violation de Renseignements personnels doit être signalée à la CAI.
2. Afin d'établir le risque de préjudice sérieux pour les droits et libertés et la vie privée de la personne concernée, le RPRP de l'Organisme municipal doit effectuer une analyse de risque conformément à la méthodologie d'évaluation de risque décrite dans le document intitulé à l'Analyse de risque de préjudice sérieux pour une personne concernée à l'Annexe 2 des présentes.

3. Afin de s'assurer qu'un incident de même nature ne se reproduise, le RPRP de l'Organisme municipal doit effectuer une évaluation des facteurs relatifs à la vie privée (analyse d'impact relative à la protection des Renseignements personnels) à l'égard de l'activité de traitement affectée par l'Incident de confidentialité.
4. Si l'Incident de confidentialité n'est pas susceptible d'entraîner un risque de préjudice séreux pour les personnes concernées visées, aucune notification n'est requise. Toutefois, l'Incident de confidentialité doit être enregistré dans le registre des Incidents de confidentialité.
5. La CAI doit être informée dans un délai raisonnable, mais au plus tard dans les 72 heures selon les normes établies par l'Organisme municipal. Toute raison éventuelle de retard au-delà d'un délai diligent doit être communiquée à la CAI.

Le RPRP enverra des notifications à la CAI qui comprendront les éléments suivants :

1. Le nom de l'organisme ayant fait l'objet de l'Incident de confidentialité.
2. Une description de la nature de l'atteinte.
3. Les catégories de Renseignements personnels concernées ou, si cela n'est pas possible, la raison justifiant l'impossibilité de fournir une description desdits Renseignements personnels.
4. Le nombre approximatif de personnes concernées.
5. Les mesures que l'Organisme municipal a prises ou entend prendre afin d'aviser les personnes concernées dont un Renseignement personnel est concédé par l'incident ainsi que la date à laquelle les personnes concernées ont été avisées ou le délai envisagé pour les aviser.
6. Le nom et les coordonnées du chef d'équipe d'intervention en cas d'Incident de confidentialité.
7. Les conséquences de l'incident de confidentialité, y compris une description des éléments qui amènent l'Organisme municipal à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées (sensibilité des Renseignements personnels concernés, différentes utilisations malveillantes possibles desdits Renseignements personnels et probabilité de leur usage à des fins préjudiciables).
8. Les mesures prises pour remédier à l'Incident de confidentialité et éviter que de nouveaux incidents de même nature ne se produisent ainsi que le délai où les mesures ont été prises ou le délai d'exécution envisagé.
9. Toute information relative à l'Incident de confidentialité, y compris notamment sa cause et ses circonstances, la date ou la période où l'incident a eu lieu ou une approximation de cette période, la date ou la période au cours de laquelle l'Organisme municipal a pris connaissance de l'Incident de confidentialité.
10. (Le cas échéant,) une mention précisant qu'une personne, une entreprise ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la CAI à l'égard de la surveillance de la protection des Renseignements personnels a été avisé de l'incident.

Le Règlement sur les incidents de confidentialité, A-2.1, r. 3.1 détermine le contenu et les modalités des avis qui doivent être transmis à la CAI et aux personnes concernées.

L'avis à la CAI doit contenir les informations suivantes :

SECTION II

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

3. L'avis à la Commission d'accès à l'information qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, donné en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé(chapitre P-39.1), est fait par écrit et doit contenir les renseignements suivants:

1° le nom de l'organisation ayant fait l'objet de l'incident de confidentialité et, le cas échéant, le numéro d'entreprise du Québec qui lui est attribué en vertu de la Loi sur la publicité légale des entreprises (chapitre P-44.1);

2° le nom et les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident;

3° 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;

4° une brève description des circonstances de l'incident et, si elle est connue, sa cause;

5° la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

6° la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;

7° le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;

8° une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, telle 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;

9° les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;

10° les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que la date ou la période où les mesures ont été prises ou le délai d'exécution envisagé;

11° le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

4. L'organisation doit transmettre à la Commission d'accès à l'information tout

renseignement énoncé à l'article 3 dont elle prend connaissance après lui avoir transmis l'avis qui y est visé. L'information complémentaire doit alors être transmise avec diligence à compter de cette connaissance.

Quand un Incident de confidentialité présente le risque d'un préjudice sérieux, l'Organisme municipal doit aviser par écrit la CAI. Un **formulaire d'avis** doit être transmis à la CAI aux coordonnées suivantes :

Commission d'accès à l'information
525, boulevard René-Lévesque Est, Bureau 2.36
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741 – Sans frais : 1 888 528-7741 – Télécopieur : 418 529-3102
Courrier électronique : cai.communications@cai.gouv.qc.ca

Le formulaire peut être téléchargé à cet endroit : https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FO_Incident_Conf.pdf

Suivant l'envoi de son formulaire d'avis, si l'Organisme municipal prend connaissance de nouvelles informations, elle doit s'empresser de les communiquer à la CAI.

L'Organisme municipal doit également tenir un Registre des incidents de confidentialité à jour. À la demande de la CAI, l'Organisme municipal doit transmettre une copie de son registre. Les renseignements du registre doivent être mis à jour et conservés pour une période minimale de cinq (5) ans, après la date ou période de prise de connaissance de l'Incident de confidentialité par l'Organisme municipal.

ANNEXE 4 : ÉVALUATION APPROFONDIE DE L'INCIDENT DE CONFIDENTIALITÉ ET PRÉVENTION

Dans son évaluation approfondie de l'incident de confidentialité, le RPRP doit notamment :

- Au besoin, approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des mesures prises face à cet incident, incluant les dates et les intervenants concernés;

- Vérifier si les normes, politiques ou directives internes en vigueur au moment de l'incident, tant sur le plan de la sécurité de l'information que de la protection des renseignements personnels, ont été suivies par les personnes impliquées – déterminer 1) les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant, et 2) si celles-ci doivent être bonifiées à la lumière de l'incident survenu;

- S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;

- Au besoin, formuler des recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;

- S'assurer de la réelle nécessité, pour l'organisme, de la collecte des renseignements personnels concernés;

- Le cas échéant, prévoir le suivi devant être accordé.

ANNEXE 5 : SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL