Plessisville

Administration

POLITIQUE MUNICIPALE N 26

EN MATIÈRE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

TABLE DES MATIÈRES

1. Objet

La présente politique a pour but de baliser et standardiser le processus de gestion des incidents de confidentialité qui peuvent survenir à la Ville de Plessisville en conformité avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

2. Abréviations

Dans la présente politique, on entend par :

CAI	Commission de l'accès à l'information du Québec
Loi sur l'accès	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1).
Ville	Ville de Plessisville
RPRP	Responsable de la protection des renseignements personnels

3. Définition

Incident de confidentialité	Tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même que la perte d'un renseignement personnel ou toute autre atteinte à la protection du renseignement.

4. Champs d'application

La présente politique s'applique à l'ensemble du personnel de la Ville, y compris les gestionnaires, les membres de comités et les stagiaires. Elle s'applique également à tous les fournisseurs et tiers qui détiennent des renseignements personnels appartenant à la Ville.

5. Rôles et responsabilité des différents intervenants

Employé	Un employé qui découvre ou soupçonne l'existence d'un incident doit aviser immédiatement par écrit le responsable de la protection des renseignements personnels.
Tiers	Toute personne détenant des renseignements personnels appartenant à la Ville et qui découvre ou soupçonne l'existence d'un incident doit aviser

immédiatement, par écrit, le responsable de la protection des renseignements personnels de la Ville.

RPRP : Le responsable doit veiller au respect de la Loi sur l'accès et à sa mise en œuvre au sein de la Ville. Il doit être le point de contact principal des communications relatives à l'incident et s'assurer du respect des obligations légales de la Ville à l'égard de l'incident.

6. Procédure d'intervention

Le RPRP doit effectuer les étapes suivantes pour respecter les exigences légales prévues aux articles 63.8 à 63.11 de la *Loi sur l'accès*. Les étapes qui suivent peuvent être réalisées simultanément.

A. Identification

Tout employé qui découvre ou soupçonne l'existence d'un incident doit en aviser immédiatement le RPRP. Si des rencontres doivent avoir lieu suivant l'incident, la présence à ces rencontres et tous les documents en découlant doivent être limités aux seules personnes nécessaires à la résolution de l'incident.

B. Évaluation initiale de la situation

Pour évaluer un incident, le RPRP doit déterminer les éléments suivants :

- Les renseignements compromis;
- Les personnes concernées;
- La cause et la portée de l'incident;
- Le risque de préjudice lié à cet incident.

Le RPRP doit effectuer une évaluation initiale de tous les incidents qui lui sont rapportés à l'aide du formulaire d'évaluation et de suivi des incidents de confidentialité joint à l'annexe A de la présente politique. Au cours de l'évaluation initiale, le RPRP doit attribuer un degré de gravité à l'incident potentiel en fonction du tableau de classement des incidents, joint à l'annexe B. Certains des facteurs ne s'appliquent pas nécessairement à tous les incidents. Si un incident présente des caractéristiques qui correspondent à plusieurs colonnes de gravité, la gravité de l'incident correspond à la gravité la plus élevée. Le classement des incidents et l'évaluation de la situation sont un processus dynamique. La gravité d'un incident peut évoluer au fur et à mesure que l'enquête révèle de nouveaux détails. L'évaluation faite par le RPRP ne lie aucunement la Ville et ne constitue pas une conclusion ou un aveu de quelque nature.

C. Enquête

Le RPRP coordonne la collecte et la préservation des éléments de preuve, afin de répondre aux questions « qui, quoi, quand, où, pourquoi et comment » à l'égard de chaque incident. L'objectif est de déterminer la cause fondamentale de l'incident, son étendue et ses effets. La Ville peut procéder à une enquête de cybersécurité et interroger tout employé ayant connaissance de l'incident.

Le RPRP assure le suivi continu de l'évaluation initial et de l'enquête afin de déterminer si quelque chose d'autre peut être fait pour mitiger les effets de l'incident et y mettre fin. Les systèmes ou les activités doivent être rétablis le plus rapidement possible, pourvu que cela n'engendre pas d'autres problèmes de sécurité, n'expose pas la Ville à un risque d'incidents additionnels ou n'entraîne pas la perte ou la destruction involontaire d'éléments de preuve. Le RPRP évalue également la possibilité de récupérer des données perdues à partir d'une copie de sauvegarde.

D. Recours à des tiers

Dans certains cas, le recours à des tiers, comme des consultants en cybersécurité, des conseillers juridiques ou des experts en technologies de l'information, peut se montrer nécessaire ou approprié.

E. Évaluation du risque de préjudice sérieux et signalement

Le RPRP doit procéder à l'évaluation du risque de préjudice. Pour ce faire, il doit prendre en compte la sensibilité des renseignements concernés par l'incident, les conséquences appréhendées de leur utilisation, la quantité de renseignements impliqués, le nombre de personnes visées et la probabilité que les renseignements soient utilisés à des fins préjudiciables.

L'annexe C donne des exemples d'éléments ayant une haute ou faible probabilité que les renseignements soient utilisés à des fins préjudiciables.

Si le RPRP conclut à la présence d'un risque de préjudice sérieux, la Ville doit alors aviser la CAI et les personnes concernées par l'incident de confidentialité. Des modèles de signalement à la CAI et aux personnes concernées se trouvent à l'annexe D de la présente politique.

F. Tenue du registre et prévention

Le RPRP doit documenter chaque incident de confidentialité qui vise des renseignements personnels en tenant un registre des incidents de confidentialité qui contient notamment les informations suivantes :

- Les détails de l'incident, y compris ses causes, ce qui s'est passé et les renseignements personnels affectés;
- Les effets et les conséquences de l'incident;
- Les mesures correctives prises;
- La justification des décisions prises en réponse à l'incident, en particulier dans le cas d'un incident qui n'est pas signalé à la CAI ou aux personnes concernées.

Tous les incidents de confidentialité doivent être inscrits au registre, et cela, que le risque de préjudice soit sérieux ou non. Le RPRP révise et actualise les politiques, procédures et pratiques de la Ville en tenant compte des leçons tirées de l'enquête sur l'incident.

G. Récupération

La Ville doit mettre en œuvre les mesures appropriées, notamment :

- La réinstallation du système d'exploitation;
- La restauration des systèmes à partir de sauvegardes propres;
- La réorganisation des systèmes;
- La restriction des accès aux dossiers papier et numériques en fonction des tâches et responsabilités de chaque employé;
- Le nettoyage des fichiers si nécessaire;
- La mise à jour des routeurs ou des pare-feux si nécessaire;
- L'installation de correctifs de sécurité;
- La suppression des vulnérabilités;
- La reconnexion au réseau;
- La validation des fonctions du système.

7. 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 la Ville a pris connaissance de l'incident.

ANNEXE A : INCIDENT DE CONFIDENTIALITÉ - FORMULAIRE D'ÉVALUATION ET DE SUIVI

1. Identification de l'incident de confidentialité
Les renseignements compromis : Les personnes concernées : La cause et la portée de l'incident : Le risque de préjudice lié à cet incident :
2. Degré de gravité
Le tableau de classement des incidents, joint à l'annexe B du présent formulaire, présente divers facteurs devant aider le RPRP à classer un incident. Certains des facteurs ne s'appliquent pas nécessairement à tous les incidents. Prendre note que la gravité de l'incident correspond à la gravité la plus élevée. Degré de gravité initiale : Date : Degré de gravité : Date : Degré de gravité : Date :
3. Enquête
Collecter et préserver les éléments de preuve (à joindre au présent formulaire, le cas échéant), pour répondre aux questions suivantes :
Qui : Quoi : Quand : Où : Pourquoi : Comment :
Après avoir répondu aux questions précédentes, il faut les analyser et répondre aux questions suivantes :
La cause fondamentale de l'incident : L'étendue de l'incident : Les effets de l'incident :

Déterminer s'il y a des solutions qui peut être fait pour mitiger les effets de l'incident et y mettre fin :

Procéder à une enquête de cybersécurité : Oui ☐ Non ☐

Confier un mandat à un expert de la technologie de l'information : Oui ☐ Non ☐

Récupération de données à faire : Oui ☐ Non ☐

4. Évaluation du risque de préjudice sérieux

Questions de bases :

Les conséquences appréhendées de leur utilisation :

La quantité de renseignements impliqués :

Le nombre de personnes visées :

La probabilité qu'ils soient utilisés à des fins préjudiciables :

Facteurs de HAUT risque :

1. L'incident de confidentialité résulte d'un acte intentionnel ☐
2. Une entité malveillante ou qui présente un risque pour la réputation de la personne concernée a pris possession des renseignements personnels ☐
3. Les renseignements ont été communiqués à un nombre important de personnes ☐
4. Les renseignements n'ont pas pu être récupérés ☐
5. Les renseignements sont facilement accessibles (par exemple, en l'absence de chiffrement adéquat) ☐
6. Un préjudice s'est effectivement matérialisé ☐
7. Autres :

Facteurs de FAIBLE risque :

1. Les renseignements sont entre les mains d'entités restreintes ou connues qui se sont engagées à détruire ou ne pas divulguer les renseignements ☐
2. Les renseignements ont été exposés à des personnes ou des entités peu susceptibles de les communiquer de façon préjudiciable (par exemple, dans le cadre d'une communication accidentelle à un mauvais destinataire) ☐
3. Les renseignements compromis ou inaccessibles ont été récupérés ☐

4. Les renseignements sont adéquatement chiffrés, anonymisés ou autrement difficiles d'accès ☐

Conclusion de l'évaluation du risque de préjudice

Risque de préjudice conclu par le RPRP après l'analyse :

5. Signalement (lors d'un risque de préjudice sérieux)

Est-ce qu'un avis doit être transmis à la Commission de l'accès à l'information :

Est-ce qu'un avis doit être transmis aux personnes concernées :

Si oui, qui sont ces personnes :

Date de l'envoi des avis, si requis :

6. Tenue du registre

Est-ce que l'incident de confidentialité a été inscrit au registre :

7. Prévention

Quelles mesures la Ville a-t-elle mises en place ou devra mettre en place pour s'assurer que ce genre d'incident ne se reproduise plus :

La réinstallation du système d'exploitation ☐

La restauration des systèmes à partir de sauvegardes propres ☐

La réorganisation des systèmes ☐

La restriction des accès aux dossiers papier et numériques en fonction des tâches et responsabilités de chaque employé ☐

Le nettoyage des fichiers si nécessaire ☐

La mise à jour des routeurs ou des pare-feux si nécessaire ☐

L'installation de correctifs de sécurité ☐

La suppression des vulnérabilités ☐

Politique de gestion des incidents de confidentialité ☐

La reconnexion au réseau ☐

La validation des fonctions du système ☐

8. Commentaires

Date de finalisation de l'évaluation :

Signature de la personne responsable des incidents de confidentialité :

Le

Me Geneviève Ferland Lamontagne, greffière

ANNEXE B : FACTEURS ET DEGRÉ DE GRAVITÉ DE L'INCIDENT

Facteurs relatifs à l'incident	Degré de gravité de l'incident						
	1er degré		2e degré		3e degré		N/A justification
Effets sur les personnes concernées et les systèmes	Touche peu de personnes ou de systèmes	☐	Effet à l'échelle d'un service	☐	Effet à l'échelle de la Ville	☐	
Effet sur le public	Aucun	☐	Effet potentiel	☐	Effet indéniable	☐	
Mesures de remédiation	Solutions disponibles	☐	Faibles mesures de remédiation	☐	Aucune mesure de remédiation	☐	
Chiffrement ou anonymisation des renseignements touchés	Algorithme de chiffrement et contrôle par clés robustes	☐	Algorithme et/ou contrôle par clés faibles	☐	Aucun chiffrement, ou chiffrement facilement déchiffrable	☐	
Procédure de résolution des problèmes techniques	Disponible et bien définie	☐	Procédure de résolution mal définie, solutions disponibles	☐	Aucune procédure de résolution ni aucune autre solution disponible	☐	
Sensibilité des renseignements	Faible	☐	Moyenne	☐	Élevée	☐	
Incident devant potentiellement être	Non	☐	Possible	☐	Oui	☐	

signalé à la CAI, aux personnes concernées ou une autorité de réglementation ou agence d'application de la loi							

ANNEXE C : EXEMPLES D'ÉLÉMENTS QUI INDIQUENT UNE HAUTE OU UNE FAIBLE PROBABILITÉ QUE LES RENSEIGNEMENTS SOIENT UTILISÉS À DES FINS PRÉJUDICIABLES

Haut risque	Faible risque
L'incident de confidentialité résulte d'un acte intentionnel (par opposition à une divulgation accidentelle).	Les renseignements sont entre les mains d'entités restreintes ou connues qui se sont engagées à détruire ou ne pas divulguer les renseignements.
Une entité malveillante ou qui présente un risque pour la réputation de la personne concernée a pris possession des renseignements personnels.	Les renseignements ont été exposés à des personnes ou des entités peu susceptibles de les communiquer de façon préjudiciable (par exemple, dans le cadre d'une communication accidentelle à un mauvais destinataire).
Les renseignements ont été communiqués à un nombre important de personnes.	Les renseignements compromis ou inaccessibles ont été récupérés.
Les renseignements n'ont pas pu être récupérés.	• Les renseignements sont adéquatement chiffrés, anonymisés ou autrement difficiles d'accès.
Les renseignements sont facilement accessibles (par exemple, en l'absence de chiffrement adéquat).	
Un préjudice s'est effectivement matérialisé.	

ANNEXE D : MODÈLE DE SIGNALEMENT À LA CAI D'UN INCIDENT DE CONFIDENTIALITÉ

[Madame, Monsieur],

Nous vous informons par la présente de la survenance d'un incident de confidentialité impliquant des renseignements à caractère personnel (l'« Incident », tel que plus amplement décrit ci-dessous), lequel présente un niveau [« très faible », « faible »] de risque de préjudice sérieux.

1. L'Incident

1.1 Description de l'Incident et des personnes concernées

[À compléter : Par exemple : type d'incident; date de l'incident; nombre et type de personnes concernées par la violation tels que des citoyens, des partenaires, etc.].

1.2 Les renseignements personnels visés par l'Incident

[À compléter : Par exemple : quantité de renseignements personnels visés, type de renseignements, tels que le nom, les coordonnées; renseignements sensibles tels que les renseignements de santé].

2. Points de contact

Me Geneviève Ferland Lamontagne
Ville de Plessisville
1700, rue Saint-Calixte
Plessisville (Québec) G6L 1R3
gferlandlamontagne@plessisville.quebec

3. Mesures prises par la Ville de Plessisville pour aviser les personnes concernées par l'Incident

[NTD : à compléter].

4. Mesures prises par la Ville de Plessisville pour atténuer les risques de préjudice et éviter la reproduction d'incidents similaires

À ce jour, la Ville de Plessisville a pris les mesures suivantes [NTD : à compléter/modifier] :

- Courriels des employés bloqués et modifications de tous les mots de passe;
- Ordinateur de l'employé saisi et profil reconfiguré;
- Enquête, y compris la nomination du soussigné en tant que coach en matière d'incidents de confidentialité et consultant en cybersécurité.

[Madame, Monsieur],

Comme vous le savez, la Ville de Plessisville a déployé un vaste programme de protection des renseignements personnels.

Malgré les efforts déployés, ce programme n'a pu empêcher [NTD : description de l'incident en langage clair et simple, y compris la date de l'incident]. Puisque vos renseignements personnels étaient concernés [NTD : description des renseignements personnels visés par l'incident], nous avons jugé essentiel de vous aviser de cette situation et des mesures mises en place pour y remédier.

Dès que nos services ont eu connaissance de cette situation [NTD : insérer la date], ils ont pu [NTD : préciser ce qui a été fait pour mettre fin à l'incident].

Consciente de l'importance d'une telle situation, la municipalité a rapidement mis en place des mesures, afin de maîtriser, voire contenir, les risques d'éventuelles conséquences néfastes. Nous avons ainsi activement mobilisé nos services informatiques afin d'opérer une vérification approfondie de nos serveurs internes. Nos services informatiques effectuent également un contrôle manuel des ordinateurs et des disques durs, afin de vérifier que [NTD : indiquer la menace à éliminer]. [NTD : description des mesures prises pour remédier à la violation ainsi que des mesures de prévention].

De votre côté, vous pouvez également réduire les risques en [NTD : description des mesures que les personnes concernées pourraient prendre pour réduire le risque de préjudice qui pourrait résulter de l'Incident ou pour atténuer ce préjudice].

La Commission d'accès à l'information du Québec a également été avisée.

Si vous avez des questions, veuillez nous contacter à l'adresse suivante :

Me Geneviève Ferland Lamontagne, greffière
Ville de Plessisville
1700, rue Saint-Calixte
Plessisville (Québec) G6L 1R3
gferlandlamontagne@plessisville.quebec

Nous sommes conscients des perturbations que cette situation pourrait vous occasionner. Pour cette raison, nous vous adressons nos plus sincères excuses. Soyez assurés que le respect de la confidentialité des renseignements

personnels est une priorité pour la Ville de Plessisville et que nous renforcerons nos mesures pour empêcher qu'un tel incident ne se reproduise.

VILLE DE PLESSISVILLE
PROVINCE DE QUÉBEC
CANADA

EXTRAIT DU PROCÈS-VERBAL

Séance ordinaire du conseil de la Ville de Plessisville, tenue ce 5e jour du mois de septembre 2023, aux heure et lieu habituels des séances du conseil, à laquelle étaient présents les membres du conseil:

Martin Nadeau, Valérie Desrochers, Sylvain Beaudoin, Marc Morin et Jean-Félipe Nadeau.

Formant quorum avec et sous la présidence du maire, monsieur Pierre Fortier.

RÉSOLUTION NO 266-23

Adoption de la politique municipale no 26

ATTENDU QU'en vertu de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* les organismes publics se sont vu attribuer de nouvelles responsabilités en matière de protection des renseignements personnels;

ATTENDU QUE les articles 63.8 à 63.11 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* établissent des définitions, des rôles et responsabilités quant à la gestion des incidents de confidentialité;

ATTENDU QU'un incident de confidentialité est défini selon la Loi comme l'accès, l'utilisation ou la communication non autorisés à un renseignement personnel, à la perte d'un renseignement personnel ou tout autre atteinte à la protection d'un tel renseignement;

ATTENDU QUE la Ville de Plessisville juge important de se doter de règle de gouvernance à ce sujet;

ATTENDU QUE cette politique a pour but de baliser et standardiser le processus de gestion des incidents de confidentialité qui peuvent survenir à la Ville de Plessisville en conformité avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;

Proposé par monsieur Jean-Félipe Nadeau

Appuyé par monsieur Marc Morin

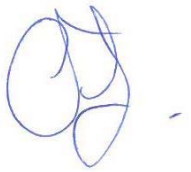
Et résolu à l'unanimité

D'ADOPTER la politique municipale nº 26 intitulée « En matière de gestion des incidents de confidentialité » laquelle demeure annexée à la présente résolution pour en faire partie intégrante.

A D O P T É E

Donné à Plessisville, ce 6e jour du mois de septembre 2023

La greffière,



Me GENEVIÈVE FERLAND LAMONTANGE