POLITIQUE ADMINISTRATIVE

Service du greffe et des affaires juridiques

POLITIQUE RELATIVE À LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Septembre 2023

TABLE DES MATIÈRES

1. PRÉAMBULE

La présente Politique vise à encadrer les exigences à respecter ainsi que les mesures à prendre en cas d'incident de confidentialité, le tout en conformité avec 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* (RLRQ c. A-2.1).

Cette Politique vise à détailler les étapes à accomplir pour assurer la gestion des incidents de confidentialité et notamment leur enregistrement au registre des incidents de confidentialité, l'évaluation du risque de préjudice sérieux, de même que le suivi à faire et les mesures correctives à prendre pour chacun des incidents de confidentialité.

2. DÉFINITIONS

« Incident de confidentialité »:	Désigne toute consultation, utilisation ou communication non autorisées par la loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce renseignement.
« Loi »:	Désigne la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1.
« Renseignement personnel »:	Désigne toute information qui concerne une personne physique et qui permet de l'identifier directement – soit par le recours à cette seule information – ou indirectement – soit par combinaison avec d'autres informations.
« Renseignement personnel sensible » :	Renseignement, qui par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison de son contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée.

3. RÔLES ET RESPONSABILITÉS

3.1 Direction des affaires juridiques

a) Élaborer les procédures, outils et documents de formation en lien avec la gestion des incidents de confidentialité et la protection des renseignements personnels;

b) Assurer la gestion et le suivi du Registre des incidents de confidentialité au comité d'accès à l'information et à la protection des renseignements personnels, de même que le suivi de l'application des mesures correctives;

c) Coordonner et participer à l'élaboration des mesures correctives en collaboration avec les directions et services concernés;

d) Assurer la formation et le soutien des employés et des cadres en matière de protection des renseignements personnels et de gestion des incidents de confidentialité.

3.2 Service des technologies de l'information

a) Participer au suivi du Registre des incidents de confidentialité en collaboration avec le comité d'accès à l'information et à la protection des renseignements personnels;

b) Participer à l'élaboration des documents de formation en matière de renseignements personnels et de gestion des incidents de confidentialité pour les systèmes d'information;

c) Participer à l'élaboration des mesures correctives pour les systèmes d'information;

d) Assurer le support auprès des employés en matière de protection des renseignements personnels dans les systèmes d'information.

3.3 Direction et autres services

a) Signaler les incidents de confidentialité;

b) Participer à l'élaboration et à l'application des mesures correctives pour les activités et systèmes d'information relevant de leur direction ou service.

4. DÉCLARATION ET ENREGISTREMENT D'UN INCIDENT DE CONFIDENTIALITÉ

4.1 Toute personne qui constate un incident de confidentialité doit, dès que possible, aviser le RPRP à l'adresse courriel greffe@ville.laprairie.qc.ca .

L'avis doit faire mention de la date de l'incident et préciser les détails entourant l'évènement. Tout document pertinent lié à l'incident doit être joint au courriel.

4.2 Autant que possible, la personne prend immédiatement les mesures nécessaires afin de contenir l'incident, d'en limiter les dommages ou d'en diminuer les risques.

4.3 Dès la réception du courriel, le RPRP crée un dossier numérique pour l'incident signalé.

L'étape de validation de l'incident à l'article 5 permettra de déterminer s'il s'agit véritablement d'un incident de confidentialité.

4.4 Chaque dossier d'incident signalé doit être identifié par l'appellation du dossier soit [inc] pour [Incident de confidentialité], suivi de l'année en cours et du numéro de dossier, selon une numérotation séquentielle.

Identification du dossier	Exemple
incaaaa_numéro séquentiel unique	inc2023-001

4.5 Le RPRP inscrit la déclaration de l'incident au Registre des incidents avec les informations qui sont disponibles, et ce, le plus rapidement possible à partir de la connaissance de l'incident.

Au besoin, il sera possible de compléter les informations manquantes ultérieurement.

5. VALIDATION DE L'INCIDENT DE CONFIDENTIALITÉ

Le RPRP doit analyser l'évènement rapporté conformément à l'article 4 afin de déterminer s'il s'agit effectivement d'un incident de confidentialité. Pour ce faire, il doit se poser les questions suivantes :

a) Les informations qui font l'objet de l'incident sont-elles des renseignements personnels, tel que définis à l'article 2 ?

b) Les renseignements personnels ont-ils fait l'objet :
   1) d'une consultation par une personne/entité non autorisée à en prendre connaissance ?
   2) d'une transmission à une personne/entité non autorisée à les recevoir ?
   3) d'une utilisation à des fins non autorisées par la loi ou par le titulaire de ces renseignements ?
   4) d'une perte ou d'un vol dans des circonstances telles que les éléments ci-haut mentionnés soient possibles ?

Pour les situations où la réponse est négative aux questions a) et b), il ne s'agit pas d'un incident de confidentialité. Aucune action particulière ne doit être prise. Toutefois, considérant les circonstances, le RPRP peut décider d'effectuer un diagnostic afin d'évaluer si les mesures de sécurité mises en place sont fonctionnelles et bien adaptées aux circonstances.

Pour toute situation où les réponses aux questions a) et b) affirmatives, il s'agit d'un incident de confidentialité. Le RPRP doit poursuivre avec les étapes subséquentes de la Politique.

6. ÉVALUATION DU RISQUE DE PRÉJUDICE

6.1 Le RPRP doit évaluer le risque qu'un préjudice soit causé à une personne concernée par le renseignement personnel visé par l'incident de confidentialité. Pour ce faire, le RPRP devra notamment répondre aux questions suivantes :

Quand l'incident a-t-il eu lieu ?
Quand l'incident a-t-il été constaté ?
Où l'incident a-t-il eu lieu ?
Quelles sont les causes probables de l'incident ?
Qui peut avoir eu accès aux renseignements personnels

Pour évaluer le risque de préjudice il faut également considérer :

1. La sensibilité du renseignement personnel concerné;
2. Les utilisations malveillantes possibles;
3. Les conséquences appréhendées de son utilisation;
4. La probabilité qu'il soit utilisé à des fins préjudiciables.

6.2 La grille d'évaluation du risque de préjudice sérieux (annexe 1) doit être complétée pour chacun des incidents de confidentialité et enregistrée dans le dossier numérique de l'incident.

6.3 Suite à l'évaluation, inscrire la réponse dans le Registre des incidents de confidentialité afin d'identifier s'il y a un risque de préjudice sérieux.

6.4 S'il n'existe pas de risque de préjudice sérieux, poursuivre avec les étapes de l'article 8.

6.5 S'il existe un risque de préjudice sérieux, aviser la personne concernée et déterminer si la Commission d'accès à l'information (ci-après « CAI ») et le public doivent être avisés.

Pour déterminer si la CAI et le public doivent être avisés, doivent être pris en considération : la sensibilité des renseignements personnels, les conséquences appréhendées de leur utilisation et la probabilité que ces renseignements soient utilisés à des fins préjudiciables.

1) Pour les incidents dont la majorité des facteurs évalués sont de 1er degré, aucun avis n'est nécessaire.

2) Pour les incidents dont la majorité des facteurs évalués sont de 2ème degré, la personne concernée doit être avisée.

3) Pour les incidents dont la majorité des facteurs évalués sont de 3ème degré, la personne et la CAI doivent être avisés.

7. TRANSMISSION D'AVIS

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

7.1 Avis à la Commission d'accès à l'information

Un avis doit être transmis avec diligence à la CAI. Le modèle d'avis est disponible sur le site internet de la CAI à l'adresse : https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf.

7.2 Avis à toutes les personnes concernées

Un avis doit être transmis par écrit, dans les meilleurs délais, aux personnes concernées.

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 Ville de l'envoi d'un avis à chacune des personnes concernées, sauf dans les cas suivants :

1) La transmission de l'avis peut causer un plus grand préjudice à la personne concernée;

2) La transmission de l'avis représente une difficulté excessive pour la Ville;

3) La Ville n'a pas les coordonnées de la personne concernée.

Dans le cas où la transmission d'un avis à la personne concernée 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, la Ville n'a pas l'obligation de transmettre un tel avis.

8. APPLICATION ET SUIVI DES MESURES CORRECTIVES ET PRÉVENTIVES

Selon les circonstances de chaque incident, le comité sur l'accès analyse les mesures correctives déployées et met en place toute autre mesure corrective ou préventive, en collaboration avec les ressources responsables.

Au minimum, le RPRP décrit et inscrit les mesures correctives mises en place dans le Registre des incidents de confidentialité.

Au besoin, le comité sur l'accès élabore un plan d'action, en assure l'application et le suivi et mesure l'efficacité d'application des mesures correctives et préventives.

Le suivi des incidents de confidentialité et du Registre des incidents de confidentialité est réalisé lors de chaque rencontre du comité sur l'accès à l'information et de protection des renseignements personnels.

9. ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur le 22 septembre 2023.

Annexe 1 - Grille d'évaluation du risque de préjudice sérieux

Facteurs relatifs à l'incident	Degré de gravité de l'incident			ÉVALUATION DU RISQUE – SECTION À COMPLÉTER
	1er degré	2ème degré	3ème degré	
Effets sur les personnes ou les systèmes	Touche peu de personnes ou de systèmes	Effet à l'échelle du service	Effet à l'échelle de la municipalité	
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 personnels	Algorithme de chiffrement et contrôle par clé robuste	Algorithme et/ou contrôle par clé faible	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	
Présence de renseignements sensibles • Renseignements d'identité • Renseignements financiers • Renseignements médicaux • Renseignements intimes • Autres renseignements qui suscitent un haut degré d'attente raisonnable de vie privée	Renseignements confidentiels non sensibles	Un seul renseignement sensible	Deux renseignements sensibles et plus	
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, diffamation, discrimination) • Répercussions sur la santé physique ou psychologique (stress) • Conséquences négatives sur le dossier de crédit	Aucune	Un seul élément	Deux éléments et plus	

• Perte d'emploi ou perte d'occasions d'emploi				
Quelle est la probabilité que ces renseignements soient utilisés à des fins préjudiciables? • L'incident résulte d'un acte intentionnel; • Les renseignements ont été exposés à des personnes ou des entités susceptibles de les communiquer de façon préjudiciable; • Les renseignements ont été communiqués à un grand nombre de personnes; • Les renseignements n'ont pas pu être récupérés ou éliminés; • Les renseignements sont facilement accessibles (par exemple en l'absence d'une protection adéquate); • Un préjudice s'est effectivement matérialisé.	Nulle ou faible	Un seul élément	Deux éléments et plus	
Incident à signaler à la CAI, aux personnes concernées ou à une autorité de réglementation ou agence d'application de la loi	Non	Possible	Oui	Inscrire cette réponse dans le registre des incidents de confidentialité