MRC des Pays-d'en-Haut

PROCÉDURE POUR LES INCIDENTS DE CONFIDENTIALITÉ

Table des matières

1. Préambule

La présente procédure est adoptée conformément aux articles 63.8 à 63.11 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*[1]

2. Objectifs

La procédure indique la marche à suivre en cas d'incident de confidentialité impliquant un renseignement personnel détenu par la MRC des Pays-d'en-Haut.

3. Définitions

Termes	Définitions
CAI	Commission d'accès à l'information
Incident de confidentialité	Accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection[2].
Loi sur l'accès	*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*
MRC	Municipalité régionale de comté des Pays-d'en-Haut
Préjudice sérieux	Un acte ou un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable.[3]
Renseignements personnels	Renseignements qui concernent une personne physique et permettent de l'identifier.[4]
Renseignement sensible	Un renseignement est considéré comme sensible lorsqu'il dévoile une information personnelle, unique ou que sa diffusion peut causer des conséquences négatives pour la personne concernée. Par exemple, le groupe ethnique, les croyances philosophique ou religieuse, la santé ou l'orientation sexuelle ou les renseignements financiers sont des informations sensibles.[5]

4. Champ d'application

La présente procédure s'applique au conseil de la MRC, la direction générale, un cadre, l'ensemble des employés et les fournisseurs de la MRC des Pays-d'en-Haut.

Toutes ces personnes doivent collaborer avec le responsable de la protection des renseignements personnels dans le cadre de l'application de la présente procédure.

5. Responsable de la protection des renseignements personnels

La responsable de la protection des renseignements personnels de la MRC est la personne suivante :

Noms	**Coordonnées**
Mme Mylène Perrier, Directrice générale	dg@mrcpdh.org (450) 229-6637 ext. 122
Me Mélissa Bergeron-Champagne, Directrice du service du greffe et greffière-trésorière adjointe.	mbergeron-champagne@mrcpdh.org 450-229-6637 ext. 124

[1] RLRQ c. A-21
[2] *Ibid,* Art. 63.9
[3] Gouvernement du Québec, *Incident de confidentialité*, en ligne : Incident de confidentialité | Gouvernement du Québec (quebec.ca) (consulté le 10 janvier 2023)
[4] o*p. cit, 1,* Art. 54
[5] Commission d'accès à l'information du Québec, *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, 2021, p. 19

6. Comité d'accès à l'information

Conformément à la Loi sur l'accès, le comité d'accès à l'information a été constitué lors de la séance du conseil du 16 août 2022 et ses membres sont les personnes suivantes[6] :

- Directeur général;
- Responsable de l'accès aux documents et de la protection des renseignements personnels;
- Directeur adjoint du parc immobilier et des technologies de l'information; et
- Greffière adjointe.

Conformément à l'article 8.1 de la Loi sur l'accès, le comité se compose de la personne responsable de l'accès aux documents et de la protection des renseignements personnels et de toute personne dont l'expertise est requise, incluant, le cas échéant, le responsable de la sécurité de l'information et le responsable de la gestion documentaire.

Le comité relève du directeur général de la MRC et celui-ci peut modifier en tout temps la composition de ses membres.

7. Marche à suivre

Lorsqu'une personne à un motif de croire qu'un incident de confidentialité est survenu, celle-ci doit compléter immédiatement le formulaire à l'annexe A de la présente et le remettre à l'un des responsables de la protection des renseignements personnels de la MRC. En cas d'absence, le formulaire peut être transmis à un membre du comité d'accès à l'information de la MRC.

Exemples d'incidents de confidentialité :

- Communication par erreur des renseignements personnels à un mauvais destinataire;
- Un vol de dossier ou de données au moyen de divers moyens technologiques (clé USB, piratage, etc.);
- Accès à des renseignements personnels par une personne non autorisée.

La procédure pour les incidents de confidentialité comprend plusieurs étapes, lesquelles sont présentées ci-dessous, celles-ci peuvent être réalisées simultanément.

7.1 Évaluer les risques

L'évaluation des risques consiste à identifier les circonstances de l'incident, cibler les renseignements personnels visés, les personnes concernées et identifier le problème. Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

Afin d'apprécier le risque engendré par l'incident de confidentialité, il faut s'interroger sur le niveau d'impact que cet événement aura sur la ou les personne(s) concernée(s), notamment en analysant les éléments suivants :

- La quantité des renseignements;
- La nature des renseignements;
- La sensibilité des renseignements;
- La gravité et la nature du préjudice sur la vie d'une personne (exemple: impacts sévères sur la vie personnelle ou professionnelle, sur les finances, procédures juridiques pour résoudre la situation) ;
- Le nombre de personnes touchées potentiellement;
- Le profil des personnes touchées (Exemple : enfants, personnes en situation d'handicap, immigrants, etc.).

Ainsi, il y a lieu de se mettre dans la peau de la ou les personne(s) concernée(s) afin de déterminer l'importance du risque en fonction de ces conséquences[7] . Le tableau ci-dessous établit les différents niveaux d'impacts afin d'apprécier l'impact d'un risque :

[6] La Liste des personnes occupant ces postes ainsi que leurs coordonnées sont indiquées dans la note administrative jointe à la fin de la présente procédure.

Niveaux	Descriptions
Très faible ou inexistant	Le risque n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne
Faible	Le risque engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes.
Grand	Le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes.
Très grand	Le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes.
Inacceptable	Le risque engendre des conséquences trop importantes ou implique une non-conformité aux lois.

Il est également possible d'effectuer l'analyse sur la base de la probabilité de la survenance d'un événement :

Probabilités	Descriptions
Très faible ou inexistant	Le risque n'a aucune chance de se concrétiser.
Faible	Le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit.
Grand	Le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelques reprises.
Très grand	Le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises.

Dans tous les cas, le niveau du risque engendré par l'incident de confidentialité est intimement lié aux informations personnelles divulguées, les personnes visées par cet incident et leurs attentes vis-à-vis du traitement de ces informations par notre organisme.

7.2 Diminuer les risques d'un préjudice

Afin de diminuer les risques d'un préjudice, il faut analyser la sensibilité du renseignement, les conséquences appréhendées et la probabilité de l'utilisation à des fins préjudiciables[8]

La personne divulguant un incident de confidentialité est invitée à formuler une solution afin de diminuer les risques d'un préjudice dans le cadre de cet incident.

7.3 Déterminer la nature du préjudice

De concert avec l'un des responsables de la protection des renseignements personnels, il y a lieu de déterminer la nature du préjudice. Ainsi, il faut considérer :

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

Dans la mesure où il y a conclusion d'absence de préjudice sérieux, le déclarant et l'un des responsables de la protection des renseignements personnels devront émettre des mesures de mitigation, tel que décrit à la section suivante.

[7] *op. cit., 5, p.9 et 10*
[8] *op. cit, 1,* Art. 63.10

Si le préjudice est considéré comme sérieux, l'un des responsables de la protection des renseignements personnels doit en aviser la CAI dans les plus brefs délais. Un modèle d'avis est disponible sur le site web de la CAI : Pour les ministères et organismes | Commission d'accès à l'information du Québec (gouv.qc.ca). 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 MRC ne peut aviser cette ou ces personne(s) si l'avis est susceptible d'entraver une enquête, représente une difficulté excessive pour la MRC ou si la MRC n'a pas les coordonnées de la personne concernée. Elle peut également aviser toute personne ou organisme susceptibles de diminuer le préjudice en lui fournissant toute information nécessaire sans le consentement de la ou les personne(s) visée(s). Cette communication devra être enregistrée et inscrite dans un registre.[9] Ce registre doit contenir les informations suivantes :

- Le nom des autres personnes ou organismes;
- Les circonstances;
- Les renseignements transmis;
- Les objectifs de cette démarche.

Ce registre est conservé par le responsable de l'accès aux documents et de la protection des renseignements personnels de la MRC. Les renseignements du registre doivent être conservés pour une période minimale de cinq ans, après la date ou la période de prise de connaissance de l'incident par la MRC.

7.4 Autres mesures de mitigation

Peu importe la nature du préjudice, le déclarant et le responsable de la protection des renseignements personnels devront soumettre au comité sur l'accès à l'information et la protection des renseignements personnels des mesures de mitigation afin de réduire les préjudices et d'éviter qu'un tel événement ne survienne à l'avenir. Le comité peut émettre des recommandations sur les mesures de mitigation proposées.

L'exécution de ces mesures relève du responsable de l'accès aux documents et la protection des renseignements personnels.

7.5 Inscription de l'incident de confidentialité

Conformément à l'article 63.11 de la Loi sur l'accès[10], tout incident de confidentialité, avec ou sans préjudice sérieux, doit être recensé dans un registre. Ce registre est conservé par le responsable de l'accès aux documents et de la protection des renseignements personnels de la MRC.

8. Modification de la politique

La présente politique 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 MRC devront en être informés afin qu'ils puissent en prendre connaissance.

9. Entrée en vigueur

Cette procédure entre en vigueur en date du 14 mai 2024.

[9] *op. cit, 1,* Art. 63.8
[10] *op. cit., 1*

ANNEXE A – DÉCLARATION D'INCIDENT DE CONFIDENTIALITÉ

DÉCLARATION D'INCIDENT DE CONFIDENTIALITÉ

INCIDENT #

INSTRUCTIONS :

Le présent formulaire doit être rempli par toute personne qui aurait des motifs de croire qu'un incident de confidentialité s'est produit.

Veuillez compléter uniquement les sections en gris. Les sections en bleues sont à l'usage unique des responsables de la protection des renseignements personnels.

INFORMATIONS

Date ou période de l'incident :	**Date ou période de la prise de connaissance de l'incident :** ☐ **Cocher s'il s'agit de la même date ou période que l'incident**

Est-ce un incident impliquant un lieu physique ou un système informatique ou technologique?

☐ **Lieu physique (locaux de la MRC, un tiers), veuillez préciser :**

☐ **Système informatique ou technologique, veuillez préciser :**

ÉVALUATION DES RISQUES **(RÉF. 7.1)**

Établir les circonstances:	
Cibler les renseignements personnels visés :	
Identification du problème :	Choisissez un élément.

Pour apprécier les niveaux d'impact, veuillez vous référer au tableau suivant :

Niveaux	Descriptions
Très faible ou inexistant	Le risque n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne
Faible	Le risque engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes.
Grand	Le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes.
Très grand	Le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes.
Inacceptable	Le risque engendre des conséquences trop importantes ou implique une non-conformité aux lois.

Quantité :

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Nature :

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Sensibilité des renseignements :

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Gravité et nature du préjudice :

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Nombre de personnes touchées :

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Profil des personnes touchées :

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Quelle est la probabilité que le risque se concrétise?

☐ **Très faible ou inexistant** ☐ **Faible** ☐ **Grand** ☐ **Très grand** ☐ **Inacceptable**

Justification :

Pour apprécier les probabilités, veuillez vous référer au tableau suivant :

Probabilités	Descriptions
Très faible ou inexistant	Le risque n'a aucune chance de se concrétiser.
Faible	Le risque a peu de chance de se

	concrétiser ou un événement similaire ne s'est jamais produit.	
Grand	Le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelques reprises.	
Très grand	Le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises.	

DIMINUER LES RISQUES D'UN PRÉJUDICE **(RÉF. 7.3)**

(À ÊTRE VALIDÉ SUBSÉQUEMMENT PAR UN RESPONSABLE DE L'ACCÈS AUX DOCUMENTS ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Sensibilité des renseignements	
Utilisations malveillantes	
Conséquences appréhendées	Choisissez un élément.
Probabilité de l'utilisation à des fins préjudiciables	
Solution :	

AUTRES MESURES DE MITIGATION AFIN D'ÉVITER UN TEL INCIDENT À L'AVENIR:

SIGNATURE

Date	**Nom du déclarant**	**Signature**

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	
SOLUTION AFIN DE DIMINUER LES RISQUES D'UN PRÉJUDICE	
NATURE DU PRÉJUDICE	
☐ **Absence de risque de préjudice sérieux**	☐ **Risque d'un préjudice sérieux**
Justifier votre position en considérant la sensibilité du renseignement, l'utilisation malveillantes possibles, les conséquences appréhendées de son utilisation et la probabilité que le renseignement soit utilisé à des fins préjudiciables :	
AVIS	
Date d'envois à la Commission d'accès à l'information	☐ **Non applicable**
<u>Personne(s) concernée(s)</u> **Est-ce que l'avis est susceptible d'entraver une enquête?** ☐ **Oui, tant que l'avis est susceptible d'entraver une enquête, aucun avis ne doit être acheminé.** ☐ **Non, inscrire la date de l'avis.**	
Est-ce qu'un avis public a été publié? ☐ **Oui, veuillez inscrire la date et justifiez la raison de sa publication** ☐ **Non**	
Est-ce qu'une personne ou un organisme est susceptible de diminuer le préjudice? ☐ **Oui, inscrire le nom de la personne ou de l'organisme et la date de l'avis** ☐ **Non**	
AUTRES MESURES DE MITIGATION AFIN D'ÉVITER UN TEL INCIDENT À L'AVENIR	
COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	
AUTRES MESURES DE MITIGATION AFIN D'ÉVITER UN TEL INCIDENT À L'AVENIR	
Date d'inscription dans le registre :	

NOTE ADMINISTRATIVE

Les membres du comité ainsi que leurs coordonnées respectives sont reproduits dans le tableau suivant :

Poste	**Nom**	**Coordonnées**
Directrice générale et Responsable de l'accès aux documents et de la protection des renseignements personnels;	Mme Mylène Perrier,	(450) 229-6637 ext. 122 dg@mrcpdh.org
Directrice du service du greffe et Responsable de l'accès aux documents et de la protection des renseignements personnels;	Me Mélissa Bergeron-Champagne,	(450) 229-6637 ext. 124 mbergeron-champagne@mrcpdh.org
Directeur adjoint du parc immobilier et des technologies de l'information	M. David Giroux	(579) 202-1722 ext. 8422 dgiroux@mrcpdh.org
Greffière adjointe	Mme Eryka Roy	(450) 229-6637 ext. 109 eroy@mrcpdh.org