Municipalité régionale de comté de L'Érable

Politique de gestion des incidents de confidentialité

Adoptée par le comité administratif le 7 février 2023 / Résolution numéro CA-2023-02-027

Rédigée par Vanessa Richer
Date prévue de révision : _____

Table des matières

Contexte 3

Objet 3

Abréviations 3

Définition 4

Champs d'application 4

Rôles et responsabilité des différents intervenants 4

Procédure d'intervention 4

1. Identification 5
2. Évaluation initiale de la situation 5
3. Enquête 6
4. Recours à des tiers 6
5. Évaluation du risque de préjudice sérieux et signalement 6
6. Tenue du registre et prévention 7
7. Récupération 7

Conservation du registre 8

Entrée en vigueur 8

Signatures 8

ANNEXE A : Formulaire d'évaluation et de suivi 9

ANNEXE B : Facteurs et degré de gravité de l'incident 14

ANNEXE C : Exemples d'éléments qui indiquent une haute ou une faible probabilité que les renseignements soient utilisés à des fins préjudiciables 15

ANNEXE D : Modèles de signalement 16

CONTEXTE

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* apporte des modifications importantes aux lois sur la protection des renseignements personnels. Sanctionnée le 22 septembre 2021, cette loi a pour objectif d'offrir un meilleur contrôle aux citoyens sur leurs renseignements personnels. Elle modernise le cadre législatif pour l'adapter à la réalité technologique d'aujourd'hui.

OBJET

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

ABRÉVIATIONS

Dans la présente politique, on entend par :

CAI :	Commission de l'accès à l'information.
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).
Loi 25 :	*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (L.Q. 2021, c. 25).
MRC :	Municipalité régionale de comté de L'Érable.
RPRP **:**	Responsable de la protection des renseignements personnels.

DÉFINITION

Incident de confidentialité **:** Un incident de confidentialité impliquant des renseignements personnels[1] se produit lorsque les renseignements personnels d'une ou de plusieurs personnes sont utilisés à une autre fin que celle prévue lors de leur collecte, qu'ils soient communiqués ou consultés sans autorisation, qu'ils soient perdus ou volés ainsi que la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

CHAMPS D'APPLICATION

La présente politique s'applique aux membres du personnel de la MRC, y compris les gestionnaires, aux membres de comités et aux stagiaires.

RÔLES ET RESPONSABILITÉ DES DIFFÉRENTS INTERVENANTS

Employé : Un employé qui découvre ou soupçonne l'existence d'un incident doit aviser **immédiatement** le responsable de la protection des renseignements personnels ou son supérieur immédiat.

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

Supérieur immédiat : Le supérieur immédiat doit aviser **immédiatement** le responsable de la protection des renseignements personnels si ce dernier n'a pas été avisé par l'employé.

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.

[1] Articles 53 à 58 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, (RLRQ, chapitre A-2.1).

1. Identification

Tout employé qui découvre ou soupçonne l'existence d'un incident doit en aviser immédiatement le RPRP ou son superviseur immédiat. Si la personne avisée n'est pas le RPRP, elle doit aviser ce dernier dès que possible.

La présence aux réunions devrait être limitée à certaines personnes et la diffusion des procès-verbaux et de tout document ou toute autre communication à l'extérieur des réunions de gestion de l'incident devrait être restreinte selon les instructions du RPRP ou du conseiller juridique.

2. 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. Le formulaire d'évaluation et de suivi des incidents de confidentialité est 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. Cette évaluation doit être révisée régulièrement au cours de l'intervention faisant suite à l'incident.

Le tableau de classement des incidents, joint à l'annexe B de la présente politique, présente divers facteurs devant aider le RPRP à classer un incident. 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. Par exemple, si un incident soupçonné touche un service ayant un lien avec des renseignements personnels (deuxième degré de gravité) et a un effet public indéniable (troisième degré de gravité), l'incident doit être classé dans la catégorie du troisième degré de gravité.

Le classement des incidents est un processus dynamique. La gravité d'un incident peut évoluer au fur et à mesure que l'enquête révèle de nouveaux détails. Le classement des incidents doit être effectué en étroite collaboration avec le conseiller juridique. Il ne lie aucunement la MRC et ne constitue aucunement une conclusion ou un aveu de quelque nature.

3. Enquête

Le RPRP, et si nécessaire de concert avec un conseiller juridique, 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 MRC pourrait devoir procéder à une enquête de cybersécurité et interroger tout employer ayant connaissance de l'incident.

4. Recours à des tiers

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

Le RPRP assure le suivi continu de l'évaluation et de l'enquête initiales 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 MRC 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.

5. 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 et le nombre de personnes visées et la probabilité qu'ils soient utilisés à des fins préjudiciables. L'annexe C indiquent 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 MRC devra alors en aviser, avec diligence, la CAI et les personnes dont les renseignements personnels sont concernés par l'incident de confidentialité.

Le RPRP et, si nécessaire le conseiller juridique, déterminent le mode et les détails de l'avis à transmettre au CAI et aux personnes concernées conformément à la Loi sur l'accès.

Des modèles de signalement à la CAI et aux personnes concernées d'un incident de confidentialité se trouve à l'annexe D de la présente politique.

6. 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 confidentialités doivent être inscrit 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 MRC en tenant compte des leçons tirées de l'enquête sur l'incident.

7. Récupération

La MRC doit mettre en œuvre les mesures correctives et de restauration appropriées, comme par exemples :

- 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 papiers 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.

CONSERVATION DU REGISTRE

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq (5) ans après la date ou la période au cours de laquelle la MRC a pris connaissance de l'incident.

ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la suite de son approbation par le comité administratif de la MRC.

SIGNATURES

Raphaël Teyssier, Directeur général
MRC de L'Érable

Date : 7 février 2023

Gilles Fortier, Préfet
MRC de L'Érable

Date : 7 février 2023

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 1 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 risques :

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 risques :

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 conclut 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 MRC a mis en place ou devra mettre en place pour s'assurer que ce genre d'incident ne réarrive pas :

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 papiers 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 confidentialités ☐ 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 _____

Vanessa Richer,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	
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 MRC	☐
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 signalé à la CAI, aux personnes concernées ou une autorité de réglementation ou agence d'application de la loi	Non	☐	Possible	☐	Oui	☐

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
Vanessa Richer
Municipalité régionale de comté de L'Érable
1783, av. Saint-Édouard
Plessisville (Québec) G6L 3S7
vricher@erable.ca

3. Mesures prises par la Municipalité régionale de comté de L'Érable pour aviser les personnes concernées par l'Incident
[NTD : à compléter].

4. Mesures prises par Municipalité régionale de comté de L'Érable pour atténuer les risques de préjudice et éviter la reproduction d'incidents similaires

À ce jour, Municipalité régionale de comté de L'Érable a pris les mesures suivantes [NTD : à compléter/modifier] :
− Courriels des employés bloqués;
− 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.

Modèle de signalement aux personnes concernées d'un incident de confidentialité

[Madame, Monsieur],
Comme vous le savez, la Municipalité régionale de comté de L'Érable 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 :
Vanessa Richer
Municipalité régionale de comté de L'Érable
1783, av. Saint-Édouard
Plessisville (Québec) G6L 3S7
vricher@erable.ca

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 Municipalité régionale de comté de L'Érable et que nous renforcerons nos mesures pour empêcher qu'un tel incident ne se reproduise.