MRC de Matawinie
Entreprenante de nature!

POLITIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LA SÉCURITÉ DE L'INFORMATION

Table des matières

Préambule

La *Loi sur l'accès aux documents des organismes publics et sur la protection de renseignements personnels* (RLRQ, c. A-2.1) (ci-après la « Loi sur l'accès ») a comme objectif d'assurer la transparence des organismes publics, tels que les organismes municipaux, et la protection des renseignements personnels.

À cet effet, dans le cadre de ses opérations courantes, la MRC de Matawinie recueille et conserve un grand nombre d'informations dont certaines revêtent un caractère sensible ou confidentiel. La MRC de Matawinie estime comme étant primordiale la protection des renseignements personnels et confidentiels qu'elle recueille et conserve.

Objectif de la politique

La présente politique a pour objectif d'assurer la sécurité des informations détenues par la MRC de Matawinie tout au long de leur cycle de vie. Elle vise en outre à fournir un cadre de gouvernance pour l'encadrement des modalités d'utilisation de circulation de l'information.

Cette politique définit comment la MRC et ses constituantes protègent les renseignements personnels et confidentiels qu'elles détiennent en précisant les normes de collecte, d'utilisation, de communication, de conservation, de droits d'accès, de rectification et de destruction.

Champs d'application

La présente politique s'applique à tous les employés de la MRC de Matawinie et ses constituantes, aux gestionnaires, aux élus ainsi qu'aux firmes externes et aux partenaires qui utilisent ou accèdent aux actifs informationnels de la MRC. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition dans le cadre de l'exécution de son travail, ou requis pour toutes autres activités de la MRC.

Cadre juridique

Le cadre juridique applicable à la présente politique est composé des lois et directives suivantes :

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1) ;
- *Loi sur les archives* (L.R.Q. c. A-21.1) ;
- *Loi sur les tribunaux judiciaires* (L.R.Q. c. T-16) ;
- *Code municipal du Québec* (L.R.Q. c.27.1) ;
- Les règlements, directives et politiques émises par la MRC de Matawinie, notamment :
  - *Le code d'éthique et de déontologie des employés de la MRC de Matawinie ;*
  - *La politique d'utilisation des technologies de l'information et des médias sociaux ;*
  - *La politique de service à la clientèle ;*
  - *La politique de télétravail*.

Définitions

Actif informationnel

Désigne une information contenant un renseignement personnel ou confidentiel, quel que soit son support ou son canal de communication, un système ou une technologie de l'information et des communications, ou un ensemble de ces éléments.

Cycle de vie de l'information

L'ensemble des étapes que franchit l'information à partir de sa création jusqu'à sa destruction et en conformité avec le calendrier de conservation de la MRC de Matawinie.

Détenteur de l'information

Toute personne qui, dans le cadre de ses fonctions, conserve de l'information que la MRC de Matawinie détient dans le cadre de ses activités.

Incident

Conséquence de la concrétisation d'un risque de sécurité de l'information. Désigne tout bris de sécurité, acte de violation des règles de sécurité, vol de données, perte de donnée, intrusion non autorisée dans le réseau, un système ou un lieu sécurisé de la MRC, la fraude, la destruction ou la négligence.

Risque de sécurité de l'information

Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information détenue par la MRC et pouvant avoir des conséquences sur la prestation de services à la population, sur la qualité de vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection de renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image de l'organisation ou du gouvernement, ainsi que sur la prestation de services fournie par d'autres organismes publics.

Renseignements personnels

Tous les renseignements qui concernent un individu et qui permettent de l'identifier directement ou indirectement, excluant les exceptions prévues par les lois applicables.

Renseignements confidentiels

Tous les renseignements qui concernent un immeuble, une personne morale ou physique relativement à de l'information que son auteur ou son propriétaire estime confidentielle, comme des informations de nature financière, commerciale ou stratégique, excluant les exceptions prévues par les lois applicables.

Sécurité de l'information

Protection résultant de l'ensemble des mesures de sécurité en place afin d'assurer la disponibilité, l'intégrité et la confidentialité de l'information détenue par la MRC.

Cadre de gestion

La mise en œuvre de la présente politique requiert la collaboration de l'ensemble du personnel et des partenaires de la MRC qui doivent assumer les rôles et responsabilités suivantes :

Direction générale

Veille à ce que les ressources humaines, techniques et financières mobilisées dans l'organisation soient adéquates pour assurer la protection des actifs informationnels et demeure imputable du respect de la mise en œuvre de la *Loi sur l'accès*.

Responsable de la protection des renseignements personnels

Veille à la protection de l'ensemble des renseignements personnels détenus par la MRC et en conformité avec les obligations édictées dans la *Loi sur l'accès* à l'égard de ces fonctions. Par défaut, ce rôle est assumé par la direction générale, mais le Conseil de la MRC peut le déléguer par résolution à un employé-cadre.

Comité d'accès à l'information et de protection des renseignements personnels

Soutient l'organisation dans l'exercice de ses obligations en vertu de la *Loi sur l'accès*, notamment en évaluant annuellement le niveau de protection des renseignements personnels détenus par la MRC, en établissant et en assurant le suivi des règles de gouvernance en matière de protection des renseignements personnels et en veillant à former les membres de l'organisation en la matière.

Gestionnaire

Veille à faire appliquer les principes directeurs contenus dans la présente politique. Doit définir les actifs informationnels détenus par leur service et participer à l'analyse des risques en matière de protection des renseignements personnels, puis s'assurer de l'exécution des contrôles mis en place.

Responsable d'un actif informationnel

Est désigné par la direction propriétaire de l'actif pour appliquer les règles de sécurité et pour gérer les risques en identifiant les menaces et les impacts possibles sur les activités de la MRC dans l'éventualité où un risque se matérialiserait. Il doit en outre veiller à informer les utilisateurs des mécanismes visant à assurer la sécurité et doit divulguer promptement tout incident de sécurité à l'égard des actifs sous sa responsabilité.

Utilisateur d'actifs informationnels

Veille à respecter les principes directeurs contenus et les encadrements prévus dans la présente politique dans le but d'assurer la protection des renseignements personnels détenus par la MRC.

Principes directeurs

1) Collecte de renseignements personnels

La collecte des renseignements par la MRC s'effectue en toute transparence avec le consentement libre et éclairé de l'utilisateur et uniquement dans le cas où la collecte d'information est nécessaire.

2) Finalité de la collecte de renseignements

La collecte de renseignements personnels est réalisée uniquement lorsqu'il en est essentiel dans les activités de la MRC et dans le but d'offrir un service personnalisé, dans les limites des lois et des règles applicables. Par conséquent, la MRC recueille et utilise dans le cadre de ses opérations des renseignements personnels pour les fins suivantes :

- Vérifier l'identité de l'usager ;
- Déterminer l'admissibilité aux services offerts par la MRC ;
- Exécuter les mandats conférés à la MRC en vertu des lois applicables ;
- Offrir un service personnalisé ;
- Suivre des requêtes auprès de la MRC et de ses mandataires ;
- Communiquer de l'information aux citoyens et partenaires qui en font la demande ;
- Élaborer des statistiques ;
- Améliorer les services offerts.

3) Consentement

Conformément aux lois applicables, la MRC de Matawinie indique clairement les fins pour lesquelles les renseignements personnels sont recueillis et demande le consentement de l'utilisateur pour en faire usage. Le consentement s'applique uniquement pour l'usage permis de sorte qu'un nouveau consentement doit être demandé pour utiliser les renseignements personnels recueillis pour une autre fin que celle convenue.

4) Détention et conservation des renseignements personnels

La MRC veille à ce que les renseignements personnels qu'elle détient soient exacts, mis à jour et conservés uniquement pour le temps nécessaire pour réaliser la fin pour laquelle ils ont été recueillis. Des règles de sécurité pour assurer la protection des renseignements personnels et confidentiels s'appliquent tout au long de leur cycle de vie.

La durée de conservation des documents contenant des renseignements personnels est déterminée conformément à la *Loi sur les archives* (chapitre A-21.1), au calendrier de conservation et au plan de classification.

5) Utilisation des renseignements personnels

L'accès aux actifs informationnels de la MRC est restreint de façon spécifique aux personnes mandatées pour exercer des fonctions pour lesquelles ces actifs ont été recueillis. Les employés affectés à des tâches leur donnant accès à des actifs informationnels doivent signer un engagement de confidentialité.

6) Droit de rectification, de retrait et de destruction

Toute personne concernée par un renseignement personnel que détient la MRC peut demander que ses renseignements personnels soient rectifiés, détruits ou qu'ils ne soient plus utilisés pour les fins auxquelles ils ont été recueillis. Pour toute demande d'accès ou de rectification d'un renseignement personnel, la personne concernée doit pour ce faire remplir le formulaire prévu à cet effet sur le site Internet de la MRC. Les renseignements personnels ou confidentiels qui, selon le calendrier de conservation, ne sont pas tenus d'être conservés seront systématiquement détruits.

7) Fin du cycle de vie des renseignements personnels

La MRC conserve les renseignements personnels pour la durée prévue après quoi, elle en assure la destruction. Les renseignements personnels périmés sont détruits ou anonymisés pour une utilisation à des fins publiques, à moins que le calendrier de la MRC ne prévoie le versement dans le fonds d'archives institutionnel. Le moyen de destruction privilégié est le déchiquetage qui est confié à une entreprise externe compétente et spécialisée dans le domaine.

8) Possibilité de porter plainte à l'égard de l'inobservation des principes

Si un individu estime qu'un principe de la présente politique n'est pas respecté, il est possible de porter plainte en s'adressant au responsable de la protection des renseignements personnels de la MRC dont les coordonnées figurent sur le site Internet de l'organisation. Le plaignant recevra un accusé de réception et une enquête interne sera déclenchée. À la suite de l'enquête, de nouvelles mesures de contrôles pourront être mises en place et un suivi sera effectué auprès du plaignant.

Sécurité de l'information

Tous les actifs informationnels de la MRC sont conservés dans un environnement sécurisé. Des mesures de sécurité adéquates sont mises en place en considérant le niveau de sensibilité des données. Seules les personnes qui, dans le cadre de leurs fonctions, doivent avoir accès à un actif informationnel précis ont l'autorisation d'y accéder.

Gestion des risques

Les actions entreprises afin de contrôler et d'assurer la sécurité des actifs informationnels sont mises en place à la suite d'une analyse tenant compte du niveau de risque et de gravité d'un incident potentiel. Une appréciation du niveau de risque des renseignements personnels détenus par la MRC est réalisée annuellement par le *Comité d'accès à l'information et de protection des renseignements personnels*, afin de considérer les modifications par rapport aux exigences liées à la sécurité de l'information.

Gestion des actifs informationnels

Au moins un responsable est nommé pour chaque actif informationnel détenu par la MRC et ce dernier collabore avec le *Comité d'accès à l'information et de protection des renseignements personnels* afin de déterminer les mesures de contrôle servant à en assurer la sécurité.

Gestion des identités et des accès

L'attribution des droits d'accès est standardisée en fonction du poste occupé pour chaque employé de la MRC en lien avec les tâches à accomplir. Tout accès supplémentaire à un actif informationnel qui n'est pas expressément inclus selon la description de fonction doit faire l'objet d'une demande au *Comité d'accès à l'information et de protection des renseignements personnels* qui évaluera le risque et la pertinence de la demande.

Acquisition et développement des logiciels et des systèmes d'information

La sécurité de l'information doit être considérée dès le début par l'initiateur d'un nouveau projet en collaboration avec le *Comité d'accès à l'information et de protection des renseignements personnels*. Les exigences relatives à la sécurité des systèmes d'information doivent être clairement identifiées, documentées, puis révisées périodiquement tout au long du cycle de vie du système.

Gestion des accès physiques

Des mesures de contrôle sont mises en place et maintenues afin de protéger les installations, les employés et les actifs informationnels contre les accès non autorisés. La gestion des accès comprend notamment un accès verrouillé en tout temps aux espaces administratifs, à la salle des serveurs, à la salle des archives ainsi qu'une directive interne sur la gestion des clés et des accès de la MRC.

Déclaration d'incidents

Un incident de confidentialité survient lorsqu'il y a accès, utilisation, communication non autorisée, perte ou toute atteinte à la protection des renseignements personnels détenus par la MRC. Tout incident de confidentialité doit être rapporté sans délai au responsable de la protection des renseignements personnels qui consignera l'incident dans un registre. Une analyse entourant l'incident est réalisée afin d'évaluer si des stratégies d'atténuation ou de contrôles supplémentaires doivent être appliquées.

Lorsque l'incident de confidentialité implique un préjudice sérieux, le responsable de la protection des renseignements personnels veille à informer la *Commission d'accès à l'information* et établit une stratégie de communication pour informer les personnes dont les renseignements personnels ont été compromis.

Mesures particulières

Sanction

Tout manquement à une règle ou un principe prévu à la présente politique est susceptible d'entraîner, sur décision de la MRC, l'application de toute sanction appropriée à la nature et à la gravité du manquement. Par conséquent, une sanction appropriée peut aller d'un simple avertissement à une réprimande, une note administrative, une suspension, un congédiement ou un recours civil.

Application, évaluation, suivi et révision

La présente politique entre en vigueur dès son adoption. Une évaluation de l'application de la présente politique sera réalisée au minimum une fois par année par le *Comité d'accès à l'information et de protection des renseignements personnels*.

HISTORIQUE DES VERSIONS

20 septembre 2023	Adoption	CM-