Régie intermunicipale de l'eau Tracy, Saint-Joseph, Saint-Roch
1200, rue Antaya
Sorel-Tracy (Québec) J3R 5G2
450 743-7087

POLITIQUES ET PROCÉDURES

Émission 2023-12-18	Révision
Responsable	Régie intermunicipale de l'eau Tracy, Saint-Joseph, Saint-Roch
Politique	Politique sur la gestion des incidents de confidentialité
Adoption	2023-12-97

POLITIQUE SUR LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ

1. ÉNONCÉ DE LA POLITIQUE

Dans le cadre de ses activités et de sa mission, la Régie intermunicipale de l'eau Tracy, Saint-Joseph, Saint-Roch, ci-après la « Régie », recueille des renseignements personnels, ci-après « Renseignement(s) personnel(s) », notamment des citoyens et de ses employés. À ce titre, elle reconnait l'importance de respecter la vie privée et de protéger les Renseignements personnels qu'elle détient.

Afin de s'acquitter de ses obligations en la matière, la Régie s'est dotée d'une Politique-cadre sur la gouvernance en matière de protection des renseignements personnels. Conformément aux exigences prévues à cette politique-cadre, la Régie met en place la présente Politique sur la gestion des incidents de confidentialité, ci-après « Politique ».

2. CHAMP D'APPLICATION

La présente Politique s'applique à tout employé ou personne qui découvre ou soupçonne l'existence d'un Incident de confidentialité et à toute personne qui procédera à une intervention à la suite d'un tel Incident.

3. OBJET

La présente Politique a pour objet de garantir une réaction rapide et adéquate lors de la survenance d'un Incident de confidentialité afin de minimiser les répercussions et prévenir la survenance d'incidents similaires.

4. CADRE NORMATIF

La présente Politique s'inscrit dans un contexte régi notamment par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1.). Conformément à cette loi, la présente Politique est accessible via le site Internet de la Ville de Sorel-Tracy.

5. DÉFINITIONS

Aux fins de la présente Politique, les termes suivants désignent :

« CAI » : la Commission d'accès à l'information du Québec.

« Incident de confidentialité » ou **« Incident »** : 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).

« Personne(s) concernée(s) » : désigne une personne physique à qui se rapportent les Renseignements personnels.

« Renseignement(s) personnel(s) » : 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.

« Responsable de la protection des renseignements personnels » ou **« RPRP »** : désigne la personne qui, au sein de la Régie, exerce cette fonction et veille à y assurer le respect et la mise en œuvre de la Loi.

6. PROCÉDURE D'INTERVENTION

6.1. Identification

6.1.1. Tout employé ou personne qui découvre ou soupçonne l'existence d'un Incident de confidentialité doit en aviser immédiatement son supérieur immédiat, le cas échéant, ainsi que le RPRP.

6.1.2. L'avis au RPRP doit lui être envoyé par courriel en utilisant le formulaire disponible en annexe.

6.1.3. Lorsque cela est possible, la personne qui a fait le signalement prend au plus vite les mesures adéquates afin de contenir l'Incident et d'en limiter les dommages.

6.2. Évaluation initiale

6.2.1. Le RPRP doit effectuer une évaluation initiale de tout Incident qui lui est rapporté. Il doit ensuite évaluer s'il y a lieu de déployer la présente Politique.

6.2.2. Pour évaluer l'Incident, le RPRP doit :

- établir les circonstances de l'Incident ;
- identifier les Renseignements personnels impliqués ;
- identifier les Personnes concernées ;
- trouver le problème, que ce soit une erreur, une vulnérabilité, etc. ;
- établir le risque de préjudice.

6.2.3. Le RPRP doit considérer plusieurs facteurs lors de son évaluation, dont les suivants:

- la sensibilité des Renseignements personnels, tels un renseignement financier ou un renseignement d'identité ;
- les conséquences appréhendées de l'utilisation de ces Renseignements comme :
    - un vol d'identité ;
    - une fraude financière ;
    - une atteinte importante à la vie privée.

- la probabilité que ces Renseignements personnels puissent être utilisés à des fins préjudiciables.

6.2.4. Si le RPRP conclut que l'Incident dénoncé n'est pas un Incident de confidentialité en vertu de cette Politique ni au sens de la Politique-cadre sur la gouvernance en matière de protection des renseignements personnels, il avise par courriel la personne qui a fait la dénonciation de son intention de ne pas y donner suite.

6.2.5. Si le RPRP conclut que l'Incident dénoncé est un Incident de confidentialité en vertu de la présente Politique ou au sens de la Politique-cadre sur la gouvernance en matière de protection des renseignements personnels, il déploie la présente Politique.

6.3. 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 Régie peut procéder à une enquête de cybersécurité et interroger tout employé ou personne ayant eu connaissance de l'Incident.

Le RPRP, s'il juge que cela est nécessaire, peut avoir recours à des tiers, tel que, mais sans limitation, des consultants en cybersécurité, des conseillers juridiques externes et des experts en technologies de l'information externe.

6.4. Diminution des risques

6.4.1. Lorsqu'un Incident de confidentialité est identifié, le RPRP doit prendre rapidement les mesures raisonnables qui s'imposent afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux Incidents de même nature ne surviennent, soit par exemple :

- cesser la pratique non autorisée ;
- récupérer ou exiger la destruction des Renseignements personnels impliqués ;
- corriger les lacunes informatiques.

6.5. Inscription de l'Incident

6.5.1. Le RPRP doit inscrire l'Incident au registre des incidents de confidentialité, et ce, que le risque soit qualifié ou non de sérieux.

6.5.2. Pour chaque Incident, les informations suivantes doivent être indiquées audit registre :

- la nature de l'Incident ;
- la cause de l'Incident ;
- la date de survenance de l'Incident ;
- la date de la découverte de l'Incident ;
- la date de la dénonciation de l'Incident au RPRP ;
- le type de Renseignement personnel impliqué ;
- le nombre de Personnes concernées ;
- les conséquences et les effets de l'Incident ;
- les moyens utilisés pour remédier à la situation et limiter les risques de préjudice ;
- la justification des décisions prises en réponse à l'Incident qui n'a pas été signalé ;
- une mention selon laquelle la situation a été notifiée à la Personne concernée et/ou au CAI;

6.6. Évaluation du risque de préjudice et signalement de l'Incident

6.6.1. Dans le cadre de son analyse, le RPRP devra notamment tenir compte des éléments suivants :

- la sensibilité des Renseignements personnels concernés par l'Incident ;
- les conséquences appréhendées de leur utilisation ;
- la probabilité qu'ils soient utilisés à des fins préjudiciables ;
- la quantité de Renseignements personnels impliqués et le nombre de personnes visées.

Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la Personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple à l'humiliation, une atteinte à la réputation, une perte financière, un vol d'identité, des conséquences négatives sur un dossier de crédit ou une perte d'emploi.

6.6.2. Si le RPRP conclut que l'Incident dénoncé ne risque pas d'entrainer un préjudice sérieux, il peut décider d'aviser toute personne dont un Renseignement personnel est concerné par l'Incident, à moins que cet avis ne soit susceptible d'entraver une enquête.

6.6.3. Si le RPRP conclut que l'Incident dénoncé risque d'entrainer un préjudice sérieux, il doit aviser dans les meilleurs délais toute personne dont un Renseignement personnel est concerné par l'Incident, à moins que cet avis ne soit susceptible d'entraver une enquête. Puis, il avise la CAI dès que possible, même s'il n'a pas colligé l'ensemble des informations relatives à l'Incident. Un délai peut s'appliquer entre le moment où la Régie prend connaissance de l'Incident et celui où le RPRP en avise les Personnes concernées. Ce délai peut être nécessaire afin, par exemple, d'identifier les Renseignements personnels impliqués, les Personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

Le RPRP peut aussi aviser toute personne ou tout organisme susceptible de diminuer ce risque. À cette fin, il ne peut lui communiquer que les Renseignements personnels qui sont nécessaires à la poursuite de cet objectif. L'obtention du consentement de la Personne concernée par les Renseignements transmis n'est pas requise. Le RPRP doit enregistrer la communication pour garder des traces documentaires de celle-ci comme : les destinataires à qui ces Renseignements ont été communiqués, les circonstances dans lesquelles les Renseignements ont été communiqués, la nature des Renseignements transmis ainsi que les objectifs de cette démarche.

6.7. Prévention

6.7.1. Le RPRP doit prendre ou veiller à ce que soit prise toute autre mesure de mitigation afin de réduire et d'éviter qu'un tel Incident ne se reproduise, par exemple :

- 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 ;
- la mise à jour des routeurs ou des pare-feux ;
- l'installation de correctifs de sécurité ;
- la suppression des vulnérabilités ;
- la reconnexion au réseau ;
- la validation des fonctions du système.

7. SANCTIONS

Toute personne qui enfreint la présente Politique est passible de sanctions selon le cadre normatif applicable.

8. MISE À JOUR

De manière à suivre l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels, la présente Politique pourra être mise à jour au besoin.

9. ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur lors de son adoption par le conseil d'administration de la Régie.

Régie intermunicipale de l'eau Tracy, Saint-Joseph, Saint-Roch
1200, rue Antaya
Sorel-Tracy (Québec) J3R 5G2
450 743-7087

AVIS DE SIGNALEMENT
D'UN INCIDENT DE CONFIDENTIALITÉ

SECTION 1 – INFORMATIONS GÉNÉRALES

Le présent formulaire doit être utilisé par tout employé de la Régie de l'eau ou personne qui désire signaler un incident de confidentialité.

SECTION 2 – IDENTIFICATION DU DÉCLARANT

Prénom	**Nom**
	Titre d'emploi, le cas échéant
Courriel	**Numéro de téléphone**

SECTION 3 – DÉTAILS RELATIFS À L'INCIDENT

Description de l'incident (contexte, cause, source) **Nombre de personnes visées :** **Type de personne visée (employé, citoyen, etc.) :**	**Date de l''incident (AAAA/MM/JJ)** **Date de la connaissance de l'incident par le déclarant (AAAA/MM/JJ)**

Nature des renseignements personnels visés par l'incident (ex : nom, adresse, N.A.S., etc.)

Support sur lequel les renseignements personnels visés se trouvaient (lettre, courriel, système de requêtes, autre plateforme, etc.)

Description des mesures qui ont été prises immédiatement après la connaissance de l'incident

S'il s'agit d'un incident technologique, est-ce que la Division des technologies de l'information de la Ville de Sorel Tracy a été avisée? Oui ☐ Non ☐

À votre connaissance, est-ce que l'incident concerne des renseignements personnels détenus par un fournisseur de services ? Si oui, lequel et identifiez une personne ressource chez ce fournisseur? Oui ☐ Non ☐

Personne ressource chez ce fournisseur :

SECTION 4 – ENVOI DU FORMULAIRE

Veuillez transmettre le présent formulaire par courriel au responsable de la protection des renseignements personnels (RPRP).

SECTION 5 – SIGNATURE

Signature	**Date (AAAA/MM/JJ)**