SAINT-CYPRIEN

POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ PHYSIQUE ET DE GESTION DES INCIDENTS

AVRIL 2024

PROVINCE DE QUÉBEC

MUNICIPALITÉ DE SAINT-CYPRIEN

MRC DES ETCHEMINS

POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ PHYSIQUE ET DE GESTION DES INCIDENTS

SÉANCE ordinaire du conseil municipal de la Municipalité de Saint-Cyprien, tenue le 9 avril 2024, à 19h00, à la salle du conseil municipal au 399, rue Principale, à laquelle étaient présents :

LE MAIRE, M. Michel Bernard

LES MEMBRES DU CONSEIL :

- M. Gilles Audet
- Mme Réjeanne Gosselin
- M. Édouard Fournier
- M. Charles Therrien
- Mme Joane Rochon
- M. Michael Mercier

Tous les membres du conseil formant un quorum.

CONSIDÉRANT QUE la Municipalité de Saint-Cyprien (ci-après la « Municipalité ») est un organisme public assujetti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A -2.1 (ci-après la « Loi sur l'accès »);

CONSIDÉRANT QUE la Municipalité s'engage à protéger les renseignements personnels qu'elle collecte et traite dans le cadre de ses activités dans le respect des lois et règlements applicables;

EN CONSÉQUENCE, LE CONSEIL DÉCRÈTE CE QUI SUIT :

OBJECTIF

La sécurité physique est essentielle pour protéger les renseignements personnels. En suivant cette politique et cette procédure, la municipalité peut minimiser les risques associés aux incidents de sécurité physiques, maximiser la protection des renseignements personnels contre les risques associés aux incidents de sécurité physiques et garantir une gestion efficace des incidents.

CHAMP D’APPLICATION

Cette politique et procédure s'appliquent à tous les employés, les bénévoles, sous-traitants et visiteurs des locaux de l'entreprise.

RESPONSABILITÉS

La personne responsable de la protection des renseignements personnels est responsable de la mise en œuvre et de la supervision de cette politique. Chaque employé est responsable de la suivre et de la respecter.

Sécurité des locaux

- Les zones sensibles, telles que les salles de serveurs, les archives et les zones de stockage, doivent être clairement identifiées et sécurisées avec des accès restreints.
- Les systèmes d'alarme doivent être installés et régulièrement testés.

Sécurité des équipements et des documents

- Les appareils portables (ordinateurs portables, téléphones intelligents, tablettes) doivent être sécurisés lorsqu'ils ne sont pas utilisés.
- Les documents contenant des renseignements personnels doivent être rangés dans des armoires verrouillables.
- Les supports de stockage (clés USB, disques durs externes) doivent être correctement étiquetés, stockés et cryptés.

Formation et sensibilisation

Tous les employés doivent recevoir une formation sur la sécurité physique et être régulièrement informés des meilleures pratiques et des mises à jour de la politique.

Gestion des incidents

- Tout incident de sécurité physique doit être immédiatement signalé à la direction ou à l'équipe désignée.
- La personne responsable des renseignements personnels doit être avisée de tout incident.
- Les incidents doivent être analysés en fonction du degré de préjudice qu'ils représentent pour les individus concernés.

- Tout incident doit être ajouté au registre d'incidents des renseignements personnels de l'organisation.
- Une procédure claire pour répondre aux incidents doit être mise en place et régulièrement mise à jour.

PROCÉDURE EN CAS D'INCIDENT

- **Identification:** Tout employé qui détecte un incident de sécurité physique doit immédiatement le signaler à la direction ou à l'équipe désignée. La personne responsable de la protection des renseignements personnels doit également toujours être avisée.

- **Évaluation:** Une fois l'incident signalé, évaluez sa gravité, sa portée et les renseignements personnels potentiellement affectés.

- **Contenir:** Prenez des mesures immédiates pour contenir l'incident.

- **Notification:** Si des renseignements personnels ont été compromis, informez les parties concernées conformément aux obligations légales.

- **Enquête:** Menez une enquête pour déterminer la cause de l'incident et mettre en place des mesures pour éviter que cela ne se reproduise.

- **Revue:** Une fois l'incident résolu, organisez une revue pour évaluer la réponse à l'incident, identifier les leçons apprises et mettre en œuvre des améliorations.

ENTRÉE EN VIGUEUR

La présente politique entre en vigueur dès son adoption par le conseil.

Copie certifiée conforme à Saint-Cyprien, le 16 avril 2024.

Stéphanie Asselin

_____

Stéphanie Asselin
Directrice générale et greffière-trésorière

Michel Bernard

_____

Michel Bernard
Maire

Adoption de la politique : 9 avril 2024
Avis de promulgation : 16 avril 2024

ANNEXE 1

REGISTRES DES INCIDENTS DE CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS

Il est obligatoire de noter tous les incidents dans votre registre des incidents de confidentialité. Le registre doit être tenu à jour et être révisé régulièrement. Les incidents de confidentialité doivent être traités de manière sérieuse et toute leçon tirée de ces incidents doit être appliquée pour améliorer les pratiques de sécurité de l'organisation.

Marche à suivre :

- **Date ou période de l'incident** : Quand l'incident a-t-il eu lieu ?
- **Description des renseignements personnels visés par l'incident** : S'ils ne sont pas connus, ajoutez la raison pour laquelle il est impossible de fournir cette information.
- **Description de l'incident** : Qu'est-ce qui s'est passé exactement ? Quels renseignements personnels ont été compromis ?
- **Nombre de personnes concernées par l'incident** : Si cette information est inconnue, veuillez ajouter une approximation de ce nombre.
- **Cause de l'incident** : Quel a été le facteur déclenchant de l'incident ? Par exemple, était-ce une attaque externe, une erreur interne, un problème technique, etc ?
- **Mesures prises en réponse à l'incident** : Qu'est-ce qui a été fait pour atténuer les effets de l'incident ? Y a-t-il eu une notification aux personnes touchées ou à la Commission d'accès à l'information ?
- **Effets de l'incident** : Quels ont été les effets sur les personnes concernées et sur l'organisation ? Y a-t-il eu des conséquences juridiques, financières ou en matière de réputation ?
- **Mesures prises pour prévenir des incidents similaires à l'avenir** : Quels changements ont été apportés à la suite de l'incident pour éviter qu'un incident similaire ne se reproduise ?

Autres actions à prendre :

- Assurez-vous de joindre votre Grille d'évaluation du risque de préjudice bien remplie à ce document pour chaque incident, il vous permettra d'identifier clairement les éléments qui vous amènent à conclure le niveau de risque de préjudice.

Date ou période de l'incident	Description des renseignements personnels visés	Description de l'incident	# de personnes concernées par l'incident	Cause de l'incident	Mesures prises en réponse à l'incident	Effets de l'incident	Mesures prises pour prévenir des incidents similaires à l'avenir

ANNEXE 2

GRILLE D'ÉVALUATION DU RISQUE DE PRÉJUDICE

Nom de la personne responsable de la protection des renseignements personnels	
Date de l'incident	
Description de l'incident	
Date de l'évaluation du risque de préjudice	

GRILLE D'ÉVALUATION DU RISQUE DE PRÉJUDICE

Critère d'évaluation	Faible	Modéré	Élevé
Sensibilité des renseignements compromis			
Conséquences appréhendées de leur utilisation			
Probabilité d'utilisation préjudiciable			

NOTES ET OBSERVATIONS

Comment utiliser cette grille:

- **Sensibilité des renseignements :** Cochez la case correspondant au niveau de sensibilité des renseignements compromis.
- **Conséquences appréhendées de leur utilisation :** Cochez la case qui correspond le mieux aux conséquences potentielles si les renseignements étaient utilisés de manière inappropriée.
- **Probabilité d'utilisation préjudiciable :** Cochez la case qui reflète la probabilité que les renseignements soient utilisés de manière préjudiciable.

- **Notes et observations :** Utilisez cet espace pour ajouter des détails ou des observations pertinentes concernant l'incident ou l'évaluation.

Une fois la grille remplie, elle doit être jointe à la documentation de l'incident et conservée conformément aux exigences de conservation des dossiers de l'entreprise et de la Loi 25.

<u>Voici quelques questions additionnelles pour vous aider à identifier le niveau de risque.</u>

1. Type d'incident

☐ Accès non autorisé
☐ Utilisation non autorisée
☐ Communication non autorisée
☐ Perte ou autre atteinte à la protection des renseignements personnels

2. Est-ce que des renseignements personnels ont été visés par cet incident ?

☐ Oui. Il s'agit d'un incident de confidentialité.
Compléter les questions subséquentes pour évaluer les risques de préjudice.

☐ Non. Il s'agit d'un incident de sécurité. Cependant, vous n'avez pas de déclaration à faire à la CAI. Inscrire l'incident au registre et continuer l'analyse pour évaluer les conséquences appréhendées et les mesures à prendre.

3. Quels ont été les renseignements visés par l'incident

☐ Renseignements d'identification
Ex. : Nom, coordonnées (adresse postale, courriel, numéro de téléphone), numéro d'assurance sociale / maladie, permis de conduire, code permanent, codes d'utilisateur, mot de passe, etc.

☐ Renseignements démographiques
Ex. : Date de naissance, origines ethniques, orientation sexuelle, identité de genre, religion, état matrimonial, niveau d'instruction, etc.

☐ Renseignements de nature financière
Ex. : Numéro de carte de crédit, de compte bancaire, information sur le soutien financier ou l'accommodation financière fournie par un établissement à un élève / un employé, salaire, conditions d'emploi, etc.

☐ Renseignements de nature médicale
Ex. Âge, taille, poids, dossiers médicaux, groupe sanguin, plan d'intervention, etc.

☐ Renseignement génétique ou biométrique
Ex. Empreintes digitales, signature vocale, ADN, etc.

☐ Autre, Préciser _____
Ex. Antécédents judiciaires, dossier d'employé, etc.

4. Les renseignements personnels visés étaient-ils protégés par un mot de passe ou chiffrés ?

☐ Oui, passez à la question 8
☐ Non, continuez l'analyse

5. Est-ce que les renseignements personnels visés par l'incident ont été récupérés ou détruits ?

☐ Oui, passez à la question 9
☐ Non, continuez l'analyse

6. Quelles sont les mesures qui ont été prises pour réduire les risques ?
Ex. Mesures de sécurité administratives, physiques, techniques, contact avec les autorités policières ou des experts externes, etc.

7. Combien de personnes sont visées (Élèves, parents, employés actuels ou antérieurs, consultants), si possible, veuillez les séparer par l'identification de chaque type de personne.

8. Des conséquences peuvent-elles néanmoins être appréhendées ?

☐ Oui, continuez l'analyse
☐ Non, vous n'avez pas de déclaration à faire à la CAI, mais vous devez inscrire l'incident au registre

9. Quelles sont les conséquences appréhendées de l'utilisation du renseignement personnel

☐ Vol d'identité
☐ Fraude financière / Impact sur le dossier de crédit

☐ Diffusion des renseignements personnels, notamment sensibles
☐ Répercussion sur la santé physique ou psychologique
☐ Perte d'emploi
☐ Humiliation, atteinte à la réputation, à la vie privée
☐ Impact sur les relations professionnelles ou d'affaires
☐ Autre, préciser _____

11. Quelles sont les probabilités de l'utilisation du renseignement personnel à des fins préjudiciables

☐ Faible
☐ Modéré
☐ Élevé

12. En fonction de cette évaluation (niveau du préjudice, du type de renseignements personnels visés, des mesures prises, de la probabilité que les conséquences appréhendées se réalisent, l'incident de confidentialité doit (plus d'un choix peut s'appliquer)

☐ Être inscrit au registre des incidents de confidentialité
☐ Être déclaré avec diligence à la CAI (formulaire Risque de préjudice sérieux dans votre Trousse ou sur le site de la CAI en cliquant ici)
☐ Être déclaré aux personnes concernées*

*Note : La personne concernée n'a pas à être avisée si cela est susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.