CANADA
PROVINCE DE QUÉBEC
M.R.C. LE DOMAINE-DU-ROY
MUNICIPALITÉ DE CHAMBORD

PROCÉDURE EN CAS D'INCIDENT DE CONFIDENTIALITÉ DE LA MUNICIPALITÉ DE CHAMBORD

PRÉAMBULE

CONSIDÉRANT QUE la Municipalité de Chambord (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;

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;

CONSIDÉRANT QUE pour s'acquitter de ses nouvelles obligations prévues à la loi, le Conseil souhaite adopter la présente Procédure en cas d'incident de confidentialité, comme prescrit par les articles 63.8 à 63.11 de la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels*, RLRQ, c. A-2.1;

EN CONSÉQUENT,

Il est proposé par XXX, appuyé par XXX et résolu à l'unanimité des conseillers **QUE** soit et est adoptée la Procédure en cas d'incident de confidentialité de la Municipalité de Chambord, et qu'il soit et est ordonné et statué par la présente Procédure ainsi qu'il suit, à savoir :

1. PRÉAMBULE

Le préambule ci-dessus fait partie intégrante de la présente Procédure.

2. OBJET DE LA PROCÉDURE

La présente Procédure vise à encadrer les exigences à respecter ainsi que les mesures à prendre en cas d'Incident de confidentialité, le tout en conformité avec les articles 63.8 à 63.11 de la Loi.

3. CADRE NORMATIF

La présente politique est adoptée conformément à ce qui est prévu notamment à l'article 63.11 de Loi, et est accessible par le biais de son site internet en tout temps.

Elle s'applique aux Renseignements personnels détenus par la Municipalité et à toute personne qui traite lesdits Renseignements personnels.

4. INTERPRÉTATION

À moins de stipulation expresse à l'effet contraire, les expressions, termes et mots suivants ont, dans la présente Procédure, le sens et l'application que lui attribue le présent article :

CAI : désigne la Commission d'accès à l'information;

Incident de confidentialité : désigne tout incident défini par l'article 63.9 de la Loi, à savoir tout accès, utilisation ou communication non autorisés par la Loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce Renseignement personnel;

Loi : désigne la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1;

Municipalité : désigne la Municipalité de Chambord;

Personne concernée : désigne une personne physique à qui se rapportent un ou des Renseignements personnels.

Registre : désigne le registre que la Municipalité doit mettre en place et mettre à jour conformément à ce qui est prévu à l'article 63.11 de la Loi ainsi que de l'article 7 du *Règlement sur les incidents de confidentialité*, RLRQ, c. A-2.1, r.3.1.

Renseignement personnel : désigne tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier, comme prévu à l'article 54 de la Loi. Sans limiter la portée générale de ce qui précède, constitue un Renseignement personnel en vertu de la présente politique et de la Loi :

a) **Renseignements d'identification :** Adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale, numéro d'assurance maladie, identifiant numérique, etc.;

b) **Renseignements de santé :** Dossier médical, diagnostic, consultation d'un professionnel de la santé, médicament, ordonnance, renseignement sur la cause d'un décès, etc.;

c) **Renseignements financiers :** Revenu d'une personne, renseignements relatifs à l'impôt, numéro de compte bancaire, biens possédés, numéros de cartes de crédit, etc.

d) **Renseignements relatifs au travail :** Dossier disciplinaire, motifs d'absence, dates de vacances, salaire, évaluation de rendement, etc.

e) **Renseignements relatifs à la situation sociale ou familiale :** État civil, le fait qu'une personne ait ou non des enfants, admissibilité à l'assurance-emploi, etc.

Ne constitue pas un Renseignement personnel protégé visé par la présente politique :

a) Le nom d'une Personne concernée, sauf lorsqu'il est mentionné avec un autre Renseignement personnel concernant la Personne concernée, ou lorsque sa seule mention révèlerait un Renseignement personnel sur cette personne;

b) Tout Renseignement personnel qui a un caractère public au sens des dispositions des articles 55 et 57 de la Loi;

c) Tout Renseignement personnel qui concerne l'exercice, par la Personne concernée, d'une fonction au sein d'une entreprise, tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail;

Renseignement personnel sensible : désigne tout Renseignement personnel, aux termes du troisième (3e) alinéa de l'article 59 de la Loi, qui, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée;

Responsable de la protection des renseignements personnels (RPRP) : Personne désignée afin de veiller à l'application et à la conformité des règles en matière de protection des renseignements personnels au sein de la Municipalité.

5. APPLICATION

La présente Procédure doit être appliquée dès que survient un Incident de confidentialité.

Le RPRP est responsable de voir à l'application de la présente Procédure. Dans le cadre de ses fonctions, il peut se fait assister par d'autres employés de la Municipalité. Il peut également, sous réserve des règles de gestion contractuelles et de délégation de pouvoir, utiliser des services externes spécialisés en la matière.

Tous les employés doivent collaborer avec le RPRP dans le cadre de l'application de la présente Procédure.

6. CONSTAT DE L'INCIDENT DE CONFIDENTIALITÉ

Tout employé de la Municipalité qui constate un Incident de confidentialité, de quelque façon que ce soit, qu'il soit avéré ou potentiel et peu importe le niveau de risque de préjudice pouvant en découler, doit en aviser immédiatement et sans délai le RPRP, ainsi que la direction générale, par courriel ou par téléphone.

Sans limiter la définition d'un Incident de confidentialité prévue à l'article 4, peut constituer un tel incident :

a) La communication par erreur d'un Renseignement personnel à un mauvais destinataire;

b) Le vol d'un dossier ou de données au moyen de divers moyens technologiques (clé USB, piratage, etc.)

c) L'accès à des Renseignements personnels par une personne non autorisée.

7. ANALYSE D'UN INCIDENT DE CONFIDENTIALITÉ

Dès qu'il reçoit la déclaration de la survenance d'un Incident de confidentialité, le RPRP doit sans délai analyser l'évènement rapporté afin de déterminer s'il s'agit effectivement d'un Incident de confidentialité. Selon le cas :

7.1. S'il juge que l'évènement rapporté ne constitue pas, après analyse, un Incident de confidentialité, l'analyse s'arrête à cette étape et, à sa discrétion, le RPRP peut tout de même faire le nécessaire pour évaluer si les mesures de sécurité mise en place sont adéquates et fonctionnelles; ou

7.2. S'il juge que l'évènement rapporté constitue un Incident de confidentialité, le RPRP doit se conformer à la Procédure ci-après établie.

8. ÉVALUATION DES RISQUES DE PRÉJUDICE

Lorsque le RPRP détermine qu'un évènement constitue véritablement un Incident de confidentialité, conformément à ce qui est prévu à l'article 6, il doit par la suite évaluer le risque qu'un préjudice soit causé à une Personne concernée dont un Renseignement personnel est touché par l'Incident de confidentialité.

Afin d'évaluer ce risque, le RPRP devra notamment répondre aux questions suivantes :

8.1. Quand l'Incident de confidentialité a-t-il eu lieu ?

8.2. Quand l'incident de confidentialité a-t-il été constaté ?

8.3. Où l'Incident de confidentialité a-t-il eu lieu ? (Ex. : dans les locaux de la Municipalité, chez un tiers détenant des Renseignements personnels pour la Municipalité)

8.4. Est-ce un Incident de confidentialité impliquant un lieu physique ou un système informatique ou technologique ?

8.5. Dans quelles circonstances l'Incident de confidentialité s'est-il produit ?

8.6. Quelles sont les causes probables de l'Incident de confidentialité ? (Ex. : enjeux de sécurité physique, humaine, technologique, etc.)

8.7. Quelles mesures de sécurité étaient en place et, le cas échéant, pourquoi n'ont-elles pas été efficaces ?

8.8. Qui peut avoir eu accès aux Renseignements personnels concernés par l'Incident de confidentialité ? (Ex. : Employés non autorisés, mandataires, fournisseurs, tiers, etc.)

8.9. Qui sont les Personnes concernées ? (Ex. : employés, fournisseurs, citoyens, clients)

8.10. Combien y a-t-il de Personnes concernées ou, si elles ne sont pas connues, une approximation de ce nombre ?

8.11. Quelle est la nature des Renseignements personnels visés par l'Incident de confidentialité ? (Ex. : à caractère public, Renseignements nominatifs, sensibles, etc.)

8.12. Y a-t-il un risque de préjudice sérieux pour les Personnes concernées ? Aux fins de cette évaluation, le RPRP doit notamment considérer :

a) La sensibilité du Renseignement personnel concerné;

b) Les utilisations malveillantes possibles des Renseignements personnels concernés;

c) Les conséquences appréhendées de l'utilisation des Renseignements personnels concernés;

d) La probabilité que les Renseignements personnels soient utilisés à des fins préjudiciables.

9. MISE EN PLACE DE MESURES POUR DIMINUER LES RISQUES DE PRÉJUDICES

En fonction de l'évaluation de la situation et du niveau de risque de préjudice établi conformément à l'article 8.12, le RPRP doit s'assurer que des mesures raisonnables soient mises en place afin de diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux Incidents de même nature se produisent

10. AVIS À TRANSMETTRE EN CAS D'INCIDENT DE CONFIDENTIALITÉ COMPORTANT UN RISQUE DE PRÉJUDICE SÉRIEUX

Lorsque l'évaluation à être réalisée en vertu de l'article 7 des présentes amène le RPRP à conclure à l'existence d'un risque de préjudice sérieux à l'égard d'une ou plusieurs Personnes concernées à la suite de la survenance d'un Incident de confidentialité, le RPRP doit transmettre les avis suivants, à savoir :

10.1. Avis à la CAI

Un avis doit être transmis à la CAI par le RPRP avec diligence, en fonction du modèle prescrit en Annexe A de la présente Procédure.

10.2. Avis aux Personnes concernées

Un avis doit être transmis par écrit, dans les meilleurs délais, à toute Personne concernée, le tout, conformément au modèle prescrit en Annexe B de la présente Procédure. Dans le but d'agir rapidement et de diminuer les risques de préjudice sérieux, la Municipalité peut également, à sa discrétion, publier un avis public, sans toutefois qu'elle soit exemptée d'aviser les Personnes concernées.

Toutefois, malgré ce qui précède, la Municipalité peut donner l'avis strictement au moyen d'un avis public dans l'une ou l'autre des situations suivantes :

a) Lorsque le fait de transmettre l'avis prévu à l'alinéa 1 est susceptible de causer un préjudice accru à la Personne concernée;

b) Lorsque le fait de transmettre l'avis prévu à l'alinéa 1 est susceptible de représenter une difficulté excessive pour la Municipalité;

c) Lorsque la Municipalité n'a pas les coordonnées de la Personne concernée;

Malgré ce qui est prévu à l'alinéa 1, la Municipalité n'est pas tenue d'aviser toute Personne concernée par un Incident de confidentialité, si cela est susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

11. TENUE DU REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le RPRP doit veiller à ce que le Registre, figurant en Annexe C de la présente Procédure, soit mis en place à la Municipalité et mis à jour en vertu des dispositions de la présente Procédure et de la Loi et ses règlements.

Le RPRP doit veiller à ce que tout Incident de confidentialité soit d'emblée inscrit dans le Registre, sans distinction à savoir si ledit Incident de confidentialité comporte un risque de

préjudice sérieux ou non, en fonction de ce qui est prévu à l'article 7 de la présente Procédure.

La Municipalité doit également s'assurer que le contenu du Registre soit conservé pour une période minimale de cinq (5) ans après la date ou la période au cours de laquelle la Municipalité a pris connaissance de l'Incident de confidentialité.

12. MISE À JOUR ET MODIFICATION DE LA PROCÉDURE

De manière à suivre l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels et à améliorer la gestion des Incidents de confidentialité pouvant survenir à la Municipalité, la présente Procédure pourra être mise à jour et modifiée au besoin.

La présente Procédure devra également être modifiée en fonction des changements législatifs, règlementaires, ou sur recommandation de la CAI, le cas échéant, afin de s'assurer qu'elle demeure en tout temps en conformité avec la Loi et les meilleures pratiques en cette matière.

La version la plus récente de la présente Procédure se retrouve sur le site internet de la Municipalité et devra être présentée à tous les employés de la Municipalité en cas de modification en fonction du présent article.

13. ENTRÉE EN VIGUEUR

La présente Procédure entre en vigueur et prend effet à compter de son adoption

ANNEXE A – MODÈLE D'AVIS À LA CAI

Commission d'accès à l'information du Québec

1. Identification de l'organisation concernée par l'incident de confidentialité
(Veuillez remplir la section A pour un organisme public et la section B pour une entreprise)

A. Identification de l'organisme public

Nom :	
Adresse :	
Personne à contacter relativement à l'incident	
Nom :	Fonction :
Téléphone :	Courriel :
Personne responsable de la protection des renseignements personnels ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :

B. Identification de l'entreprise

Nom :	
Adresse du siège social :	
Numéro d'entreprise au Québec (selon le Registraire du Québec) :	
Dirigeant principal	
Nom :	Titre / fonction :
Téléphone :	Courriel :
Personne à contacter relativement à l'incident ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :
Personne responsable de la protection des renseignements personnels ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :

Commission d'accès à l'information du Québec

2. Date et période de l'incident de confidentialité

Date de l'incident :	Date de découverte de l'incident :
L'incident a eu lieu sur une période de :	

3. Type d'incident de confidentialité

- ☐ Accès non autorisé par la loi à un renseignement personnel
- ☐ Utilisation non autorisée par la loi d'un renseignement personnel
- ☐ Communication non autorisée par la loi d'un renseignement personnel
- ☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

3.1 Causes et circonstances de l'incident de confidentialité

Selon le type d'incident sélectionné ci-dessus, identifiez la ou les cause(s) de celui-ci :

☐ Altération délibérée	☐ Communication accidentelle	☐ Communication délibérée sans autorisation	☐ Consultation non autorisée
☐ Cyberattaque (virus, logiciel espion, etc.)	☐ Défaillance technique	☐ Destruction accidentelle	☐ Destruction volontaire sans autorisation
☐ Divulgation accidentelle	☐ Divulgation délibérée sans autorisation	☐ Erreur humaine	☐ Hameçonnage (phishing)
☐ Ingénierie sociale	☐ Perte d'accès aux renseignements	☐ Perte de renseignements	☐ Rançongiciel
☐ Utilisation incompatible	☐ Vol de renseignements	☐ Autre Précisez :	

Selon le type d'incident sélectionné ci-dessus, décrivez les circonstances de celui-ci :

Commission d'accès à l'information du Québec

Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident :	
☐ Ordinateur de bureau	☐ Dispositif amovible électronique
☐ Papier	☐ Clé USB
☐ Serveur	☐ CD
☐ Bande sonore	☐ Téléphone portable
☐ Infonuagique (cloud)	☐ Tablette
☐ Vidéosurveillance	☐ Ordinateur portable
☐ Photo	☐ Autre Précisez :

4. Description des renseignements personnels visés par l'incident de confidentialité

☐ Nom ☐ Prénom	☐ Adresse du domicile	☐ Date de naissance ou ☐ Année ☐ Mois ☐ Jour ☐ Âge
☐ Numéro de téléphone au domicile	☐ Numéro du cellulaire	☐ Adresse courriel personnelle
☐ Numéro de permis de conduire	☐ Numéro d'assurance sociale	
☐ Numéro d'assurance maladie	☐ Numéro de passeport	
☐ Salaire	☐ Fonction / occupation	
☐ **Renseignements sur des employés**, clients ou bénéficiaires Précisez :		
☐ Renseignements médicaux Précisez :		
☐ Renseignements génétiques Précisez :		
☐ **Renseignements** scolaires / académiques Précisez :		
☐ **Renseignements** bancaires / numéro de compte / institution / placements / hypothèque Précisez :		

Commission d'accès à l'information du Québec

☐ Numéro de carte de crédit	☐ Numéro d'identification personnel (NIP)	☐ Nom du détenteur	☐ Code de sécurité à trois chiffres
☐ Numéro de carte de débit	☐ Numéro d'identification personnel (NIP)	☐ Nom du détenteur	

☐ Autres renseignements personnels

Précisez :

☐ Impossible de fournir une description des renseignements personnels visés

Expliquez :

5. Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employés, de clients, d'étudiants, de patients, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens :

6. Évaluation par l'organisation du fait qu'un risque de préjudice sérieux puisse être causé aux personnes concernées par l'incident de confidentialité

Décrivez les éléments amenant l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées. Ce risque peut être attribuable au fait qu'il s'agisse de renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables. Dans ce cas, indiquez les conséquences appréhendées de leur utilisation sur les personnes concernées.

Commission d'accès à l'information du Québec

Décrivez les raisons qui supportent l'existence d'un risque de préjudice sérieux pour les personnes concernées par l'incident.

Le responsable de la protection des renseignements personnels de votre organisation a-t-il été consulté pour procéder à l'évaluation du risque de préjudice?

◯ Oui ◯ Non

7. Avis de l'organisation aux personnes concernées
(Vous pouvez joindre une copie de l'avis transmis aux personnes concernées)

L'organisation a-t-elle avisé les personnes concernées par l'incident de confidentialité?

◯ Non
◯ Oui. L'avis a été fait par :

☐ Lettre transmise par courrier	☐ Courriel	☐ Message texte
☐ Verbal (ex. par téléphone)	☐ En personne	☐ Autre Précisez :

Date de l'avis :

Si les personnes concernées n'ont pas encore été avisées, quelles mesures seront prises par l'organisation afin de le faire?

☐ Lettre transmise par courrier	☐ Courriel	☐ Message texte
☐ Verbal (ex. par téléphone)	☐ En personne	☐ Autre Précisez :

Date de l'avis prévu :

☐ Aucune notification de l'incident aux personnes concernées n'est prévue.
Expliquez :

Commission d'accès à l'information du Québec

7.1 Contenu de l'avis aux personnes concernées

Sélectionnez les éléments contenus dans l'avis transmis aux personnes concernées par l'organisation.

- ☐ Une description des renseignements personnels visés par l'incident
- ☐ Une brève description des circonstances de l'incident
- ☐ La date ou la période où l'incident a eu lieu
- ☐ Une brève description des mesures que l'organisation a prises ou entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé
- ☐ Les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice
- ☐ Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident

Y a-t-il des personnes concernées par l'incident qui ne seront pas avisées par l'organisation?

- ◯ Non.
- ◯ Oui. Combien :

  Expliquez :

7.2 Avis public aux personne concernées

L'avis aux personnes concernées a-t-il été fait, exceptionnellement, au moyen d'un avis public?

- ◯ Non
- ◯ Oui. Sélectionnez la raison applicable :
  - ☐ Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée.

    Expliquez :
  - ☐ Le fait de transmettre l'avis est susceptible présenter une difficulté excessive pour l'organisation.

    Expliquez :
  - ☐ L'organisation n'a pas les coordonnées des personnes concernées.

    Expliquez :

Commission d'accès à l'information du Québec

Par quels moyens l'avis public a-t-il été fait?
☐ Un avis dans les médias Précisez lesquels : Date de diffusion :
☐ Un communiqué de presse Date de diffusion :
☐ Un avis sur le site Web de l'organisation
☐ Une conférence de presse Lieu : Date :
☐ Une publication diffusée dans les médias sociaux Précisez lesquels :
☐ Autre Précisez :
Est-ce que l'organisation a avisé d'autres autorités de protection des renseignements personnels à l'extérieur du Québec?
☐ Commissaire à la protection de la vie privée du Canada
☐ Office of the information and privacy commissioner of Alberta
☐ Office of the information and privacy commissioner of British Columbia
☐ Commissaire à l'information et à la protection de la vie privée de l'Ontario
☐ Autre. Précisez :

Commission d'accès à l'information du Québec

8. Obligation de diminuer le risque de préjudice

Quelles mesures ont été prise dès la découverte de l'incident, notamment afin de réduire les risques de préjudice aux personnes concernées?

Dans quel délai ces mesures ont-elles été prises?

Est-ce que des mesures ont été prises après la découverte de l'incident afin d'éviter que de nouveaux incidents de même nature se reproduisent?

- ◯ Non
- ◯ Oui. Précisez :

Y a-t-il des mesures prévues qui n'ont pas encore été prises?

- ◯ Non
- ◯ Oui. Précisez :

Indiquez la date de mise en place des mesures prévues :

Une organisation doit transmettre à la Commission tout renseignement relatif à l'incident de confidentialité dont elle prend connaissance après lui avoir transmis le présent avis. L'information complémentaire doit alors être transmise dans les meilleurs délais à compter de cette connaissance.

Est-ce que des informations supplémentaires seront transmises à la Commission concernant l'incident rapporté?

- ◯ Non
- ◯ Oui. Précisez lesquelles et indiquez l'échéancier prévu :

Commission d'accès à l'information du Québec

9. Signature	
Prénom :	Nom :
Fonction :	Lieu / Ville :
Date de transmission du formulaire à la Commission :	
Pour le compte de : ◯ l'organisme ◯ l'entreprise	
Je déclare que les renseignements concernant l'incident de confidentialité fournis dans la présente déclaration sont complets et conformes aux faits.	
Signature :	

ANNEXE B – MODÈLE D'AVIS À LA PERSONNE CONCERNÉE

Madame, Monsieur,

La Municipalité de Chambord conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, tient à vous informer de la survenance d'un incident de confidentialité concernant vos renseignements personnels suivants :

[description ou énumération des renseignements personnels ou des motifs justifiant l'impossibilité de les décrire].

L'incident de confidentialité a eu lieu au sein de notre service de , le ou vers le lequel a été découvert le . Les circonstances entourant cet incident se résument comme suit : *[brève description des circonstances de l'incident]*.

Actuellement, la Municipalité prend les mesures nécessaires afin de diminuer le risque qu'un préjudice vous soit causé, les mesures suivantes sont ou seront rapidement mises en place :

- Avis à la Commission d'accès à l'information en date du ;
- *[Énumérer les mesures et dates de mise en place]*.

Afin de diminuer ou atténuer le risque qu'un préjudice vous soit causé, nous vous suggérons de prendre les mesures suivantes :

- *[Énumérer les mesures à adopter par la personne concernée]*

Pour toute information complémentaire, vous pouvez contacter le responsable de la protection des renseignements personnels au sein de la municipalité aux coordonnées suivantes :

Nom :
Téléphone :
Courriel :

Veuillez agréer, Madame, Monsieur, nos salutations distinguées.

_____
Nom
Responsable de la protection des Renseignements personnels
Municipalité de Chambord

ANNEXE C – MODÈLE DE REGISTRE D'INCIDENT DE CONFIDENTIALITÉ

Registre des incidents de confidentialité

Toutes ces informations concernent l'incident cité														
Numéro	**Renseignements visés** *(description ou si l'information n'est pas connue, indiquer la raison justifiant l'impossibilité de fournir une telle description)*	**Circonstances** *(brève description)*	**Date / Période approximative**	**Date de prise de connaissance**	**Nombre de personnes concernées** *(exact ou approximatif)*	**Risque - Préjudice sérieux**			**Transmission** *(si risque de préjudice sérieux)*					**Mesures prises par l'organisation afin de diminuer les risques qu'un préjudice soit causé**
									Date de l'avis					
									CAI	**Personne concernée**	**Public**			
						Oui	*Non*	*Motifs*			*Oui*	*Non*	*Si oui, indiquer les raisons*	