PROTOCOLE DE NOTIFICATION EN CAS D'ATTEINTE À LA VIE PRIVÉE

LOI SUR LE DROIT À L'INFORMATION ET LA PROTECTION DE LA VIE PRIVÉE (LDIPVP)

VILLE DE DIEPPE

1. INTRODUCTION

Une **atteinte à la vie privée** se produit lorsque des renseignements personnels sont recueillis, utilisés, consultés, divulgués ou éliminés d'une manière ne respectant pas les dispositions prévues par la *Loi sur le droit à l'information et la protection de la vie privée* (LDIPVP) ou, le cas échéant, la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé* (LAPRPS), à savoir les lois du Nouveau-Brunswick sur la protection de la vie privée que la Ville de Dieppe doit respecter. Pour en savoir plus sur ces lois, consultez la politique de confidentialité de la Ville.

2. OBJECTIF

Le protocole de notification en cas d'atteinte à la vie privée précise les étapes que doivent suivre les employés, les membres du conseil et les non-employés de la Ville en ce qui a trait à la détermination, à la documentation, à l'intervention et au signalement appropriés de toute atteinte présumée ou avérée à la vie privée. Ce protocole doit être lu en même temps que la politique de notification en cas d'atteinte à la vie privée de la Ville qu'il a pour objectif de soutenir.

3. PROTOCOLE DE NOTIFICATION EN CAS D'ATTEINTE À LA VIE PRIVÉE

(1) Dès la prise de connaissance d'une atteinte à la vie privée, des mesures immédiates doivent être mises en œuvre. Toute personne soupçonnant la présence d'une telle atteinte doit immédiatement la signaler à son superviseur et au secrétaire municipal.

(2) Quatre étapes doivent être suivies en cas d'atteinte à la vie privée. Elles sont décrites en détail dans le présent protocole :

1. Limitation de l'atteinte à la vie privée et évaluation préliminaire ;

PRIVACY BREACH REPORTING PROTOCOL

RIGHT TO INFORMATION AND PROTECTION OF PRIVACY ACT (RTIPPA)

CITY OF DIEPPE

1. INTRODUCTION

A **privacy breach** occurs whenever personal information is collected, used, accessed, disclosed, or disposed of in ways that are not in accordance with the provisions of RTIPPA or, when applicable PHIPAA, the NB privacy legislation to which the City of Dieppe must comply. For more information on this legislation, consult the Corporate Privacy Policy.

2. OBJECTIVE

This privacy breach response protocol details the steps that must be taken by City's employees, councillors and non-staff personnel in relation to identifying, documenting and appropriately reporting and responding to suspected or actual privacy breaches. It should be read in conjunction with, and is intended to support, the City's Privacy Breach Reporting Policy.

3. PRIVACY BREACH RESPONSE PROTOCOL

(1) Upon learning of a privacy breach, immediate action should be taken. Any person suspecting a breach must immediately notify their supervisor and the City Clerk.

(2) There are four steps that must be followed when responding to a privacy breach, which are described in detail in this protocol:

1. Breach containment and preliminary assessment;

2. Enquête et détermination des détails de l'atteinte ;

3. Notification des intervenants internes et (le cas échéant) externes concernés.

4. Évaluation des risques et mesures correctives

Remarque : Pour la plupart, ces étapes sont menées simultanément ou en séquence rapide.

1. Limitation de l'atteinte à la vie privée et évaluation préliminaire

Toute personne responsable d'une atteinte présumée ou avérée à la vie privée ou découvrant une telle atteinte doit, en consultation avec son superviseur ou le secrétaire municipal, le cas échéant, prendre des mesures immédiates pour limiter, atténuer et corriger les préjudices causés par ladite atteinte. Ces mesures peuvent notamment consister à :

a) arrêter la pratique non autorisée;

b) sécuriser tous les renseignements;

c) récupérer les copies papier de tous renseignements personnels ayant été divulgués;

d) s'assurer qu'aucune copie des renseignements personnels n'a été faite ou n'est conservée par la personne qui n'était pas autorisée à les recevoir, et à se procurer les coordonnées de la personne en question dans le cas où un suivi serait nécessaire;

e) déterminer si l'atteinte à la vie privée permet un accès non autorisé à d'autres renseignements personnels (p. ex. un système d'information électronique) et à prendre toutes les mesures nécessaires et adaptées (p. ex. modifier les mots de passe ou éteindre

2. Investigation/identifying details of the breach;

3. Notification of appropriate internal and (where appropriate) external stakeholders;

4. Risk assessment and corrective measures

Note: Many of these steps need to be carried out simultaneously or in quick succession.

1. Breach Containment and preliminary assessment

An individual who is responsible for or who discovers an actual or suspected breach must, in consultation with their supervisor and / or the City Clerk as required, take immediate steps to contain, minimize and remedy the damage from the breach. This could include for example:

a) stopping the unauthorized practice;

b) securing all information;

c) retrieving the hard copies of any personal information that has been disclosed;

d) ensuring that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtaining the individual's contact information in the event that follow-up is required;

e) determining whether the privacy breach would allow unauthorized access to any other personal information (e.g., an electronic information system) and taking whatever necessary steps are appropriate (e.g., change

temporairement un système);

f) appeler, si un courriel ou une télécopie ont été envoyés à la mauvaise personne, le destinataire pour lui demander de détruire de manière sécuritaire le document en question et tout imprimé ou toute copie ayant pu être produits;

g) signaler immédiatement, si un appareil contenant des données électroniques a été volé, ledit vol au service de gestion des TI.

2. Enquête sur l'atteinte et évaluation préliminaire

Dès qu'il a été informé d'une atteinte présumée ou avérée, le secrétaire municipal, en consultation avec le superviseur, lance immédiatement une enquête, notamment en recueillant tous les faits liés à ladite atteinte. Cette enquête consiste notamment à :

a) déterminer la nature des renseignements personnels ayant subi l'atteinte ainsi que les détails relatifs à la manière dont les données ont été perdues ou atteintes, y compris la cause apparente;

b) consigner la date et le lieu de l'atteinte à la vie privée;

c) consigner la date à laquelle l'atteinte à la vie privée a été découverte pour la première fois;

d) déterminer la portée et l'ampleur apparentes de l'atteinte (combien de personnes sont touchées, environ? Combien de dossiers ont été atteints? L'atteinte concernait-elle des renseignements d'employés, de clients ou d'autres personnes?);

e) mener un entretien avec les personnes disposant de renseignements pertinents

passwords and/or temporarily shut down a system);

f) If an email or fax is sent to the wrong person, the employee must call the recipient and ask them to securely destroy the document and any printouts/copies that were made;

g) If an electronic data device is stolen the employee must notify IT management immediately.

2. Breach Investigation / Preliminary Assessment

Upon being notified of a suspected or actual breach, the City Clerk, in consultation with the supervisor, will immediately undertake an investigation, including gathering all facts relating to the breach. This will include:

a) Identifying the nature of the personal information that is the subject of the breach, and the details surrounding how the data was lost or breached, including the apparent cause;

b) Documenting the date and location of the breach of privacy;

c) Documenting the date the breach of privacy was first discovered;

d) Identifying the apparent scope and magnitude of the breach (approximately how many people are affected? How many records have been breached? Did the breach involve employees, customers or other individuals' information?);

e) Interviewing individuals with information relevant to the breach

à propos de l'atteinte et consigner les autres renseignements pertinents;

f) préserver les renseignements personnels en question et se procurer des exemplaires de toute la documentation pertinente (copies écrites, électroniques ou enregistrements) en lien avec l'atteinte.

Le formulaire modèle de notification d'une atteinte à la vie privée doit être rempli à ce stade (se reporter à l'annexe A).

3. Évaluation des risques et mesures correctives

a) ***Évaluation des risques***

Le superviseur responsable du secteur d'activité concerné doit, en consultation avec le secrétaire municipal, examiner en profondeur la cause de l'atteinte et l'ampleur des préjudices ou des préjudices potentiels subis par les personnes touchées et les autres en conséquence de ladite atteinte.

La réalisation d'une évaluation des risques faisant suite à une atteinte à la vie privée doit tenir compte :

i) de l'évaluation des préjudices potentiels; (se reporter au TABLEAU 1)

ii) de la probabilité d'apparition des préjudices potentiels. (se reporter au TABLEAU 2)

Les tableaux 1 & 2 doivent être consultés pour faciliter la détermination des préjudices potentiels pour les personnes en conséquence d'une atteinte à la vie privée et de la probabilité d'apparition de ces préjudices potentiels. Les atteintes à la vie privée comprenant un ou plusieurs facteurs dans la colonne de droite des tableaux (risque plus élevé) peuvent généralement être décrites comme

and documenting other pertinent information; and

f) Preserving the PI in question and obtaining all copies of all relevant documentation (written, electronic or recordings) related to the breach.

The Breach Notification template should be completed at this stage (see Appendix A).

3. Risk Assessment and Corrective Measures

a) ***Risk Assessment***

The supervisor responsible for the business area in question must, in consultation with the City Clerk, fully investigate the cause of the breach and the extent of harm or potential harm brought upon the affected individual(s) and others as a result of the breach.

Completing a risk assessment when a privacy breach occurs must consider:

i) the assessment of the potential harm; (see CHART 1)

ii) The likelihood of the potential harm(s) occurring. (see CHART 2)

The Charts 1 and 2 should be consulted for guidance in identifying the potential harm to individuals resulting from a privacy breach and the likelihood of the identified harm(s) occurring. Privacy breaches involving one or more of the factors in the right most (higher risk) columns of the charts can generally be described as being of higher risk than

présentant un risque plus élevé que celles ne comprenant que des facteurs de la colonne du milieu (risque moins élevé). Le préjudice potentiel et le risque évalué pour chaque atteinte dépendront des circonstances.

b) ***Déterminer les mesures correctives requises***

À ce stade, des mesures correctives doivent être définies en vue de remédier à l'atteinte et, le cas échéant, de trouver et de résoudre la cause profonde de l'atteinte en déterminant les problèmes systémiques ou récurrents et les stratégies d'atténuation, notamment :

i) la mise en place de mesures visant à réduire le préjudice pour les personnes;

ii) une vérification des mesures de sécurité techniques et physiques;

iii) un examen des politiques et des procédures et la recommandation de révisions reflétant les leçons apprises grâce à l'enquête;

iv) un examen des pratiques de formation des employés et la proposition de recommandations;

v) un examen des pratiques existantes chez les partenaires et les agents assurant la prestation de services;

vi) toute autre mesure jugée appropriée par le secrétaire municipal au vu des circonstances.

c) ***Suivi des employés et des non-employés***

La communication avec les employés et les non-employés est essentielle après

breaches involving only those factors outlined in the middle (lower risk) columns. The potential for harm and the assessed risk of each breach will depend on the circumstances involved.

b) ***Identify Required Corrective Measures***

At this stage, corrective measures should be identified to remedy the breach and where applicable, to identify and address the root cause of the breach, identifying any systemic / recurring issues and appropriate mitigation strategies such as:

i) Providing measures to reduce the harm to individuals;

ii) An audit of the technical and/or physical security;

iii) A review of policies and procedures and recommended revisions to reflect the lessons learned from the investigation;

iv) A review of employee training practices and recommendations;

v) A review of the existing practices of service delivery partners and agents; and

vi) Any other measures considered by the City Clerk to be appropriate in the circumstances.

c) ***Employee and Non-staff Personnel Follow-up***

Communication with employees and non-staff personnel following a breach is

une atteinte à la vie privée. Le contenu et l'ampleur de cette étape varieront, mais elle doit toujours comprendre un examen de la cause de l'atteinte et des mesures à prendre pour atténuer toute atteinte future. Dans certains cas inhabituels, les employés peuvent faire l'objet de mesures disciplinaires, qui seront déterminées au cas par cas en tenant compte de toutes les circonstances.

Les non-employés seront tenus pour responsables par l'entremise du gestionnaire compétent, conformément à leur contrat conclu avec la Ville.

4. Notification des intervenants

a) Notification

Toute personne soupçonnant la présence d'une atteinte doit immédiatement la signaler à son superviseur et au secrétaire municipal.

Peu après que l'étape 1 a été accomplie, et dans certains cas simultanément, le superviseur ou le secrétaire municipal doit notifier les personnes concernées de l'incident aussi rapidement que possible, et notamment :

i) en informant la haute direction et le conseil de l'incident, le cas échéant;

ii) en s'assurant que le service de gestion des TI est informé de l'atteinte si un système d'information est concerné par cette dernière;

iii) en informant le personnel des communications qui peut être en mesure d'offrir son aide dans la communication avec les intervenants et la notification des parties externes, le cas échéant;

essential. The content and extent of this step will vary, but should always include a review of the cause of the breach and steps to be taken to mitigate future occurrences. In unusual cases, employees may be subject to disciplinary action, which will be determined on a case by case basis, taking all relevant circumstances into account.

Non-staff personnel will be held accountable through the appropriate Manager in accordance with their contract with the City.

4. **Notification of stakeholders**

a) Notification

Any person suspecting a breach must immediately notify their supervisor and the City Clerk.

Soon after completing step 1, and in some cases concurrently with these steps, the supervisor and/or City Clerk must notify implicated persons of the event at the earliest opportunity, including:

i) Advising executive management and briefing council of the event, as appropriate;

ii) Ensuring that IT management is made aware of the breach if an information system is involved;

iii) Advising Communications staff who may be able to provide assistance in communications with stakeholders and notifying external parties, as appropriate;

iv) en informant tout superviseur dont le service (y compris le personnel) pourrait interagir avec le secteur de programme subissant l'atteinte ou lui fournir un soutien;

v) en informant les ressources humaines, si une atteinte volontaire ou délibérée de la politique de la Ville est soupçonnée.

vi) L'enquête peut également nécessiter :

- de consulter des ressources externes, comme des experts de la vie privée ou de la sécurité, des conseillers juridiques ou des fournisseurs de systèmes, le cas échéant;

- d'informer la police, si une atteinte semble concerner un vol ou toute autre activité criminelle.

b) Notification du Commissaire à l'accès à l'information et à la protection de la vie privée

Il incombera au secrétaire municipal de déterminer les cas où le Commissaire à l'accès à l'information et à la protection de la vie privée devra être informé d'une atteinte à la vie privée ;

i) La loi demande à la Ville d'informer le Commissaire de la manière prescrite par la LAPRPS « dès que les circonstances le permettent » lorsque l'atteinte à la vie privée concerne la consultation, la divulgation, l'élimination, la perte ou le vol non autorisés de renseignements personnels sur la santé soumis à ladite Loi. Les exceptions à cette règle générale sont très limitées et très précises ;

iv) Advising any supervisor whose department (including staff personnel) may interact with or provide support to the program area experiencing the breach;

v) If a willful or deliberate breach of City Policy is suspected, Human Resources must be notified.

vi) The investigation may also require:

- Consulting with external resources such as privacy or security experts, legal counsel, or system vendors if appropriate; and/or

- Notifying the police, if a breach appears to involve theft or other criminal activity.

b) *Notifying the Access to Information and Privacy Commissioner*

The City Clerk will be responsible to determine instances where the Access to Information and Privacy Commissioner must or should be notified of a privacy breach.

i) The City is required by law to notify the Commissioner in the manner prescribed by PHIPAA at the "first reasonable opportunity" if the privacy breach involves the unauthorized access, disclosure, disposition, loss or theft of personal health information subject to that Act. Exceptions to this general rule are limited and very specific;

ii) il est également considéré comme une pratique exemplaire pour un organisme public d'informer le Commissaire aussi rapidement que possible de toute atteinte à la vie privée concernant tous types de renseignements personnels. Les exceptions à cette ligne directrice peuvent comprendre les cas où les préjudices potentiels que pourrait entraîner l'atteinte et la probabilité d'apparition de ces préjudices sont évalués comme présentant un faible risque ;

iii) en cas de doute, la Ville penchera en faveur d'une notification de l'atteinte au Commissaire, lequel sera consulté pour déterminer s'il est nécessaire d'informer les personnes touchées de l'atteinte à la vie privée.

La Ville doit faire tout son possible pour signaler l'atteinte à la vie privée au Commissaire aussi rapidement que possible après son apparition, même si la Ville ne dispose pas de tous les détails concernant l'incident. Des renseignements supplémentaires peuvent suivre dans le rapport écrit de la Ville envoyé au Commissaire (si nécessaire), ou peuvent être demandés par le Commissaire.

c) ***Notification des personnes touchées***

En gardant à l'esprit le principe de transparence, en règle générale, la Ville informera les personnes touchées dans le cas d'une atteinte à leurs renseignements personnels, sauf en de rares circonstances. Il incombera au secrétaire municipal de déterminer si les personnes touchées doivent être informées de l'atteinte à la vie privée, après consultation avec le Commissaire (le cas échéant), en tenant compte de toutes les exigences législatives, des attentes raisonnables des personnes touchées (p. ex. clients, employés) et du

ii) It is also accepted best practice for public bodies to notify the Commissioner as soon as possible whenever a breach of privacy involving any type of personal information occurs. Exceptions to this guideline may include instances where the potential harms that could result from the breach and the likelihood of harms occurring are assessed as low risk;

iii) When in doubt, the City will err on the side of reporting the breach to the Commissioner, who will be consulted in determining whether it is necessary to notify impacted individuals about the breach.

The City should endeavor to report the privacy breach to the Commissioner as expeditiously as possible after the breach occurs, even if the City does not have all the details relating to the incident. Additional information may follow in the City's written report to the Commissioner (if required), or may be requested by the Commissioner.

c) ***Notifying impacted individuals***

In keeping with the principle of openness and transparency, the City will generally notify impacted individuals in the event of a breach of personal information, except in rare circumstances. The City Clerk will be responsible to determine whether impacted individuals must or should be notified of a privacy breach, after consulting with the Commissioner (where appropriate), giving consideration to any legislative requirements, the reasonable expectations of the affected individuals

niveau de risque évalué pour l'atteinte en question.

Lorsque la Ville doit, en vertu de la LAPRPS (concernant une atteinte à des renseignements personnels sur la santé), notifier le Commissaire et les personnes touchées, elle DOIT fournir les renseignements suivants en personne, par téléphone ou par écrit dès que les circonstances le permettent :

i) le nom du dépositaire (Ville de Dieppe);

ii) le nom et les coordonnées de la personne désignée par la Ville pour répondre aux questions à propos des pratiques de la Ville en matière de renseignements;

iii) une description de la nature de l'atteinte à la vie privée;

iv) la date et le lieu de l'atteinte à la vie privée;

v) la date à laquelle l'atteinte à la vie privée a été remarquée par la Ville ;

vi) Étapes à suivre pour la notification des personnes :

1) Déterminer quand et comment informer les personnes (courrier direct ou appel téléphonique, avis public, médias, Internet) ;

2) déterminer qui doit communiquer avec les personnes ou leur envoyer la notification ;

3) déterminer les renseignements que doit inclure la notification ;

4) préparer la notification, au

(e.g. customers, employees) and the level of assessed risk of the breach.

When the City is required by PHIPAA (with respect to a breach of personal health information) to give notice to the Commissioner and the individuals impacted, it MUST provide the following information in person, by telephone or in writing at the first reasonable opportunity:

i) the name of the custodian (City of Dieppe);

ii) the name and contact information of the person designated by the City to respond to inquiries about the City's information practices;

iii) a description of the nature of the breach of privacy;

iv) the date and location of the breach of privacy; and

v) the date the breach of privacy came to the attention of the City.

vi) Steps for notification of individuals:

1) Determine when and how to notify (direct mail and/or phone, public notice, media, internet);

2) Determine who should contact or send notification to the individuals;

3) Determine what should be included in the notification;

4) Prepare notification, as

besoin.

Il est souhaitable qu'au moment d'informer les personnes touchées de l'atteinte à leurs renseignements personnels, les mesures correctives disponibles leur soient également communiquées. Par exemple, si un numéro d'identification a été divulgué par erreur, un nouveau numéro d'identification sera peut-être attribué.

Les préoccupations soulevées par les personnes lorsqu'elles sont informées de l'atteinte doivent être traitées autant que faire se peut, notamment en explorant raisonnablement de possibles mesures correctives supplémentaires.

appropriate.

It is desirable that, when notifying affected individuals of the breach of their PI, that available corrective measures are also communicated. For example, if an identification number was wrongly disclosed, perhaps a new identification number will be assigned. Concerns raised by the individual upon notification should be addressed as fully as possible; including, within reason, exploring additional corrective measures.

Adoptée en conseil le 13 novembre 2012

Adopted in Council on November 13, 2012

TABLEAU 1

ÉVALUATION DU PRÉJUDICE POTENTIEL

Facteur	Préjudice potentiel faible	Préjudice potentiel élevé
Nombre de dossiers ou de personnes touchés.	Petit nombre de dossiers ou de personnes.	Grand nombre de dossiers ou de personnes.
Capacité à utiliser les renseignements pour commettre une fraude ou un vol d'identité.	Non, ou capacité limitée.	L'atteinte comprend la perte de numéros d'assurance sociale, de numéros de cartes de crédit, de numéros de permis de conduire, de numéros personnels de cartes Santé, de numéros de comptes bancaires et de toute autre information pouvant être utilisée pour commettre une fraude financière ou autre.
L'atteinte pourrait entraîner un risque de préjudice physique pour les personnes touchées.	Non	Les renseignements pourraient exposer une personne à un risque de préjudice physique ou de harcèlement.
Préjudice, humiliations, atteintes à la réputation.	Non	L'atteinte comprend des renseignements comme des dossiers sur la santé mentale, des dossiers médicaux et des dossiers disciplinaires.
Identification des personnes.	L'atteinte comprend des renseignements personnels de base comme le nom, l'adresse ou la photographie, dont la publication en tant que telle, bien qu'à l'origine d'inconvénients, n'entraînera probablement pas de préjudice important à long terme.	Oui – en plus d'autres préjudices.
D'autres préjudices peuvent en résulter.	Non	D'autres préjudices potentiels peuvent se produire, y compris, sans toutefois s'y limiter, les préjudices suivants : • pertes commerciales ou perte de possibilités d'emploi; • atteinte aux obligations contractuelles; • atteintes à venir en raison de problèmes techniques semblables.

CHART 1

ASSESSMENT OF POTENTIAL HARM

Factor	Lower Potential Harm	Higher Potential Harm
Number of records or individuals impacted	Small number of records or individuals	Large number of records; large group of individuals
Ability to use the information to commit fraud or identity theft	No or limited ability	Breach includes loss of SIN, credit card numbers, driver's license numbers, personal health numbers, bank account numbers and any other information that can be used to commit financial or other fraud.
Breach could result in a risk of physical harm to impacted individuals	No	Information could place an individual at risk of physical harm, stalking or harassment.
Hurt, humiliation, damage to reputation	No	Breach involves information such as mental health records, medical records, and disciplinary records.
Identification of individuals	Breach involves basic personal information such as name, address, picture, the release of which, by itself, while causing inconvenience, is unlikely to result in significant lasting harm.	Yes – in addition to other harms
Other harms could result	No	Additional potential harms, including, but not limited to any of the following: • Loss of business or employment opportunities • Breach of contractual obligations • Future breaches due to similar technical failures.

TABLEAU 2

PROBABILITÉ D'APPARITION DES PRÉJUDICES POTENTIELS

Facteur	Faible probabilité d'apparition des préjudices	Probabilité élevée d'apparition des préjudices
Type d'atteinte	Perte	Vol
Motif du vol ou de l'accès non autorisé (le cas échéant).	Les renseignements volés ou compromis n'étaient pas la cible du vol.	Les renseignements volés ou compromis étaient la cible du vol.
Format ou protection des données.	Par exemple, les données étaient cryptées. Elles ne sont utilisables ou accessibles que par une personne disposant de connaissances ou d'équipements informatiques très spécialisés.	Par exemple, les données n'étaient pas cryptées et sont facilement utilisables ou accessibles par toute personne disposant de connaissances faibles à modérées en informatique.

CHART 2

LIKELIHOOD OF THE POTENTIAL HARM(S) OCCURRING

Factor	Lower likelihood of harm(s) occurring	Higher likelihood of harm(s) occurring
Manner of breach	Lost	Stolen
Motive for theft or unauthorized access (if applicable)	Stolen or compromised information was not the target of the theft	Stolen or compromised information was the target of the theft.
Manner in which data was formatted or protected	E.g. Data was encrypted. Usable or accessible only to an individual with highly specialized IT knowledge or equipment.	E.g. Data was not encrypted; highly usable or accessible to any individual with low to moderate IT knowledge.

ANNEXE A

FORMULAIRE DE NOTIFICATION D'ATTEINTE À LA VIE PRIVÉE

Une atteinte à la vie privée suppose la collecte, l'utilisation ou la divulgation inappropriée de renseignements personnels contrevenant à la *Loi sur le droit à l'information et la protection de la vie privée* ou à la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé.*

Pour signaler une atteinte à la vie privée, veuillez remplir la **partie A** de ce formulaire du mieux que vous le pouvez et remettez-le immédiatement au Bureau du secrétaire municipal. Si vous n'êtes pas certain de la manière de répondre à une question, veuillez laisser le champ vierge et demander de l'aide. Veuillez ne pas inclure de renseignements pouvant être inexacts.

Veuillez **ne pas** prendre de mesures en réponse à une atteinte qui ne s'inscrivent pas dans votre domaine normal de responsabilités, sans consulter préalablement votre superviseur ou le Bureau du secrétaire municipal.

PARTIE A

Date : _____

Coordonnées

Organisme public	
Personne-ressource	
Titre	
N^{o} de téléphone	
Courriel	
Adresse postale	

Évaluation des risques

1. **Décrire la nature de l'atteinte et indiquer sa cause :**

   _____

   _____

   _____

2. **Date à laquelle l'incident s'est produit :** _____

3. **Date à laquelle l'incident a été découvert**:_____

4. **Lieu de l'incident**:_____

5. **Nombre estimatif de personnes concernées par l'atteinte**:_____

6. **Type de personnes concernées par l'atteinte** :

   Client

   Employé

   Autre : _____

7. **Renseignements personnels en cause**

   Décrire les renseignements personnels qui sont en cause (p. ex. le nom, l'adresse, le numéro d'assurance sociale, les renseignements personnels). (*N'incluez **pas** de renseignements personnels identifiables dans ce formulaire)* :

   _____

   _____

   _____

   _____

8. Notification du Bureau du secrétaire municipal et du gestionnaire

Nom du gestionnaire/superviseur avisé : _____

Date de la notification : _____

Nom de la personne avisée dans le Bureau du secrétaire municipal :_____

Date de la notification : _____

PARTIE B – À remplir en consultation avec le Bureau du secrétaire municipal

9. Mesures de sécurité existantes

Décrivez les mesures de sécurité physiques (serrures, systèmes d'alarme, etc.) et les mesures de protection de la vie privée (politiques et procédures) qui étaient en place au moment de l'atteinte à la vie privée.

_____

_____

_____

_____

10. Préjudices découlant de l'atteinte à la vie privée

Déterminer les types de préjudices qui pourraient découler de l'atteinte :

Usurpation d'identité
Non ____ Oui ____

Risque de dommage physique
Non ____ Oui ____

Préjudice, humiliations, atteintes à la réputation
Non ____ Oui ____

Pertes commerciales ou perte de possibilités d'emploi
Non ____ Oui ____

Atteinte aux obligations contractuelles
Non ____ Oui ____

Autres atteintes à la vie privée dues à des défaillances techniques similaires
Non ____ Oui ____

Manquement aux normes professionnelles ou aux normes de certification
Non ____ Oui ____

Autre (veuillez préciser) :

Processus utilisé

11. La police ou d'autres autorités ont-elles été informées?

Oui Qui a été/sera informé et quand? _____

Non Pourquoi? _____

12. Les personnes concernées ont-elles été informées?

Oui Méthode et date de notification _____

Non Pourquoi? _____

13. Décrire le processus suivi/à suivre pour aviser les personnes concernées (p. ex. indiquer qui a été/sera informé, la méthode et le contenu de la notification) :

_____

_____

_____

_____

Atténuation et prévention

14. Décrire les mesures immédiates prises pour limiter l'atteinte (p. ex. changement des serrures, arrêt des systèmes informatiques) :

_____

_____

_____

_____

15. Décrire la stratégie à long terme à adopter pour corriger la situation (p. ex. formation du personnel, élaboration ou mise à jour des politiques, établissement ou mise à jour de procédures) :

_____

_____

_____

_____

APPENDIX A

PRIVACY BREACH NOTIFICATION FORM

A privacy breach occurs when there is improper collection, use or disclosure of personal information in contravention of the *Right to Information and Protection of Privacy Act* or the *Personal Health Information Privacy and Access Act.*

To report a privacy breach, please complete **Part A** of this form to the best of your ability and submit it to the City Clerk's Office without delay. If you are unsure how to respond to a question, please leave the field blank and request assistance. Please do not include information that may be incorrect.

Please **do not** take action in response to a breach that is outside your normal scope of duties, without first consulting with your supervisor or the City Clerk's Office.

PART A

Date: _____

Contact Information

Public Body	
Contact Person	
Title	
Phone	
Email	
Mailing Address	

Risk Assessment

1. **Describe the nature of the breach and its cause:**

_____

_____

_____

2. **Date of incident(s):** _____

3. **Date incident discovered:** _____

4. **Location of incident:** _____

5. **Estimated number of individuals affected:**_____

6. **Type of individuals affected:**

Client / Customer

Employee

Other**:** _____

7. **Personal Information Involved**

Describe the type of personal information involved (*e.g.* name, address, Social Insurance number, personnel information). (*Do **not** include identifiable personal information in this form)*:

_____

_____

_____

8. Notification of City Clerk's Office and Manager

Name of Manager / Supervisor Notified: _____

Date Notified: _____

Name of Person Notified in the City Clerk's Office: _____

Date Notified:_____

PART B – To be completed in consultation with the City Clerk's Office

9. Existing Safeguards

Describe physical security (locks, alarm systems etc.) and privacy safeguards (policies & procedures) that were in place at the time of the privacy breach.

_____

_____

_____

_____

10. Harm from the Breach

Identify the types of harm that may result from the breach:

Identify theft
No ____ Yes ____

Risk of physical harm
No ____ Yes ____

Hurt, humiliation, damage to reputation
No ____ Yes ____

Loss of business or employment opportunities
No ____ Yes ____

Breach of contractual obligations
No ____ Yes ____

Future breaches due to similar technical failures
No ____ Yes ____

Failure to meet professional standards or certification standards
No ____ Yes ____

Other (specify):

Process Used

11. Have the police or other authorities been notified?

Yes Who was / will be notified and when? _____

No Why not? _____

12. Have affected individuals been notified?

Yes Form & date of notification _____

No Why not _____

13. Describe the process followed / to be followed to notify affected individuals (*e.g.* who was /will be notified, the form and content of notification):

_____

_____

_____

_____

Mitigation and Prevention

14. Describe the immediate steps taken to contain the breach (*e.g.* Locks changed, computer systems shut down, etc.):

_____

_____

_____

_____

15. Describe the long-term strategy to be adopted to correct the situation (*e.g.* staff training, policy development or update, procedural development or update, etc.):

_____

_____

_____

_____