Office municipal d'habitation de Québec

Politique sur l'accès, la sécurité de l'information et la protection des renseignements personnels

Mai 2023

Table des matières

La présente politique a été élaborée par le Comité sur l'accès à l'information et sur la protection des renseignements personnels de l'Office municipal d'habitation de Québec en y intégrant les modifications prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)* soit *la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (L.Q. 2021, c.25)*.

1. Introduction

L'Office municipal d'habitation de Québec (ci-après « l'Office») détient de l'information sur différents supports, et ce, durant tout le cycle de vie de celle-ci. Cette information est nécessaire et a une importance stratégique pour le déroulement des activités de l'Office.

Toute information détenue par l'Office impose que l'organisation se donne des règles concernant l'accès et la sécurité de celle-ci ainsi que la protection des renseignements personnels.

2. Objectifs de la politique

La présente politique a pour objet d'établir les principes directeurs et les lignes de conduite à suivre en matière d'accès à l'information, de protection des renseignements personnels et de sécurité de l'information, et ce, dans le respect des lois, règlements et directives gouvernementales applicables en la matière.

La présente politique est complémentaire à la politique de gestion documentaire.

3. Champ d'application

3.1 Personnes concernées

Cette politique s'adresse à tout le personnel de l'Office. Elle concerne également toutes les personnes appelées à utiliser les actifs informationnels de l'organisation ou à accéder aux renseignements personnels.

3.2 Actifs visés

Tous les actifs informationnels de l'Office sont visés par la présente politique quel que soit le support utilisé pour les conserver.

4. Cadre législatif, réglementaire et administratif

En vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1) et de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (L.Q. 2021, c.25) l'Office est tenu d'adopter et d'appliquer des mesures administratives permettant d'encadrer les privilèges, restrictions et procédures en matière d'accès à ses documents. Il doit également protéger les renseignements personnels en tenant compte de leur caractère confidentiel, de leur collecte, de leur conservation et de leur utilisation, tout en considérant aussi l'établissement et la gestion des fichiers.

5. Principes directeurs

Les principes directeurs de l'Office municipal d'habitation pour l'accès à l'information et à la protection des renseignements personnels sont :

- La collecte : l'Office doit, lorsqu'il recueille des renseignements personnels, respecter la règle de nécessité en vertu de laquelle un organisme public ne peut recueillir que les renseignements personnels qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion. En vertu de cette règle, l'Office a aussi l'obligation d'informer la personne concernée des raisons de la collecte et du traitement qui sera fait de l'information recueillie.

  La personne concernée a un droit de regard et de rectification sur les renseignements qu'un organisme public a recueillis.

- L'accès : l'Office doit limiter la circulation des renseignements personnels qu'il a recueillis. Seules les personnes qui ont besoin des renseignements dans le cadre de leurs fonctions et de leurs activités doivent y accéder.

- L'utilisation : l'Office peut utiliser des renseignements personnels à d'autres fins que celles prévues, si la personne concernée a donné son consentement ou qu'une loi l'autorise.

- La communication : dans le cas des communications autorisées par les personnes concernées, l'Office doit s'assurer que le consentement est valide et que la communication des renseignements s'effectue de manière à préserver leur caractère confidentiel.

- La détention et la conservation : l'Office doit veiller à ce que les renseignements personnels qu'il conserve soient à jour, exacts et complets, afin de servir aux fins prévues. Il doit aussi s'assurer de gérer de manière sécuritaire l'ensemble des renseignements personnels qu'il détient.

- La destruction et l'archivage : l'Office doit détruire un renseignement lorsque l'objet pour lequel il a été recueilli est accompli et que le calendrier de conservation est respecté.

Les principes directeurs de l'Office municipal d'habitation de Québec pour la sécurité de l'information sont :

- La responsabilité et l'imputabilité : l'efficacité de la sécurité de l'information exige l'attribution claire de responsabilité à tous les membres du personnel de l'Office, qu'importent leurs fonctions. Il doit permettre une reddition de comptes adéquate avec le cadre légal.

- L'évolution : les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, humains et technologiques, ainsi que l'évolution des menaces et des risques.

- L'universalité : les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale ou au sein de l'appareil gouvernemental québécois.

- L'éthique : le processus de gestion de la sécurité de l'information doit être soutenu par une prise en charge des enjeux éthiques ayant pour but d'assurer la régulation des conduites et la responsabilisation individuelle. Cette approche vise à assurer l'intégrité et l'efficacité du personnel de l'Office dans toutes ses activités, et ce, en toute circonstance.

- La sécurité de l'information numérique est basée sur des notions de disponibilité, d'intégrité, de confidentialité, d'authentification et d'irrévocabilité.

6. Orientations

6.1 Protection, utilisation et transmission des renseignements personnels

L'Office traite de manière confidentielle tous les renseignements qu'il détient. À cette fin, à chacune des étapes de la gestion de l'information, il prend des mesures de sécurité appropriées pour assurer la protection des renseignements confidentiels et personnels au sens de la Loi sur l'accès.

L'Office limite la collecte des renseignements personnels à ceux qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre de ses programmes.

L'Office veille à ce que les renseignements personnels qu'il détient soient exacts et à jour. De plus, il limite leur utilisation aux fins pour lesquelles ils ont été recueillis. Il ne les conserve que le temps nécessaire pour répondre au besoin qui avait été déterminé. L'Office restreint l'accès à ces renseignements aux seules personnes qui en ont besoin dans l'exercice de leurs fonctions.

Les renseignements personnels détenus par l'Office sont dans des fichiers qui font l'objet d'une déclaration obligatoire relative à la nature des renseignements, à leur pertinence et aux catégories de personnes qui y ont accès.

L'Office doit prendre toutes les mesures nécessaires pour assurer la confidentialité de l'information lors de la transmission de dossiers contenant des renseignements personnels. Il ne transmet ces renseignements qu'avec le consentement de la personne concernée ou, en l'absence d'un tel accord, lorsque la Loi sur l'accès le permet.

À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la transmission ou le transfert de support d'un document doivent assurer le maintien de son intégrité et, par conséquent, de sa valeur probante.

Toute communication de renseignements personnels sans le consentement de la personne concernée est évaluée au préalable afin de déterminer sa conformité avec la Loi sur l'accès. Elle est également soumise pour autorisation au responsable de la protection des renseignements personnels.

6.2 Protection de l'information et cycle de vie

L'information détenue par l'Office est essentielle à sa mission et à ses activités courantes. Elle doit également être utilisée et protégée de manière adéquate durant tout son cycle de vie. Les détenteurs des actifs informationnels sont responsables de la sécurité de ces renseignements ainsi que de l'application des directives et des mesures de contrôle de l'Office.

La protection de l'information dont l'Office dispose s'appuie sur l'engagement formel et continu de tout le personnel ainsi que des utilisateurs à protéger l'information et le support mis à leur disposition en l'utilisant avec discernement et aux seules fins prévues. De plus, toutes les personnes concernées doivent s'engager à ne pas mettre en péril l'intégrité des actifs informationnels et à préserver le caractère confidentiel de l'information.

6.3 Sécurité d'accès

Des mesures sont mises en place pour contrôler en tout temps l'accès aux locaux de l'Office et permettre d'identifier les personnes autorisées à y entrer.

L'accès au réseau local et aux systèmes d'information de l'Office doit être accordé au moyen d'un logiciel de contrôle d'accès. Ce dernier doit permettre l'accès uniquement aux personnes dûment autorisées, au moyen d'un code d'identification personnel unique et authentifié par un mot de passe.

L'attribution des accès à des systèmes d'information comportant des renseignements personnels se fait après avoir déterminé quels sont les membres du personnel dont les tâches nécessitent un tel accès.

Les équipements informatiques de l'Office doivent être protégés adéquatement contre tout accès non autorisé et contre toute perte ou dommage qui pourrait être causé de façon accidentelle ou délibérée.

L'Office peut adopter des directives pour assurer l'uniformité et la mise en œuvre des mesures de sécurité.

6.4 Intégrité de l'information et valeur juridique

L'Office doit maintenir l'intégrité de tout document ayant une valeur juridique malgré l'interchangeabilité de son support, afin de préserver son admissibilité éventuelle devant les tribunaux.

À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la transmission ou le transfert de support d'un document doivent assurer le maintien de son intégrité et, par conséquent, de sa valeur probante.

6.5 Sensibilisation et formation

L'Office doit déployer et appuyer les efforts nécessaires pour sensibiliser son personnel aux obligations et aux pratiques en matière d'accès à l'information, de la protection des renseignements personnels et de la sécurité de l'information et de la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité ainsi qu'à son rôle et à ses obligations dans le processus de protection de ces ressources. En conséquence, il doit offrir à son personnel de la formation pertinente sur ces sujets ainsi que sur les procédures de sécurité existantes et l'utilisation adéquate de l'information et des technologies de l'information dont il fait usage dans l'exercice de ses fonctions. L'Office doit également tenir à jour un registre de ses activités de sensibilisation et de formation en ces matières.

6.6 Destruction et archivage

Conformément à son calendrier de conservation des documents, l'Office doit détruire de manière sécuritaire les actifs informationnels et les documents ne devant pas être conservés de façon permanente.

6.7 Acquisition ou développement d'applications informatiques

Les exigences en matière de protection des renseignements personnels et de sécurité de l'information doivent être prises en considération dès le début des études menant à l'acquisition ou au développement d'un système d'information. Les mesures de protection requises doivent être appliquées tout au long du processus de conception.

6.8 Évaluation des risques en sécurité de l'information

Les risques et les menaces pour la sécurité de l'information doivent faire l'objet d'évaluations périodiques. Ainsi, des mesures de sécurité doivent être mises en œuvre en fonction des risques propres à l'information et selon les risques résiduels acceptables.

6.9 Respect de la propriété intellectuelle

Tous les utilisateurs doivent se conformer aux exigences légales concernant l'utilisation des produits logiciels propriétaires ainsi que des produits, des documents et de l'information qui pourraient être protégés par des droits de propriété intellectuelle.

7. Intervenants

7.1 Responsable de la politique

Le (la) président(e) du conseil d'administration de l'Office est responsable de la présente politique. La présidente a délégué, par résolution, cette responsabilité au directeur général et au directeur de l'administration. À ce titre, ils s'assurent du respect des lois, des règlements et des directives en matière de gestion de l'information. Ils doivent principalement :

- mettre sur pied un comité sur l'accès à l'information et la protection des renseignements personnels et attribuer les rôles et responsabilités prévus à la présente politique à des membres du personnel de l'Office;
- établir un processus officiel de gestion intégrée et d'amélioration continue de la sécurité de l'information. À cet effet, une structure organisationnelle qui définit clairement les rôles et les responsabilités des employés de tous les échelons s'avère essentielle;
- veiller à ce que le personnel de direction ou d'encadrement de l'Office soit sensibilisé aux obligations de même qu'aux pratiques en matière d'accès à l'information et de renseignements personnels, et qu'ils reçoivent la formation pertinente;
- instaurer un mécanisme pour définir et évaluer les risques en matière de sécurité de l'information ainsi que pour déterminer l'adéquation des mesures de sécurité en vigueur avec ces risques.

7.2 Comité sur l'accès, la sécurité de l'information et la protection des renseignements personnels

Le comité sur l'accès, la sécurité de l'information et la protection des renseignements personnels (le comité) a la responsabilité de coordonner les activités liées à l'accès à l'information, à la protection des renseignements personnels et à la sécurité de l'information au sein de l'Office. Il suggère au directeur général les mesures particulières de protection des renseignements personnels qui devraient encadrer les projets d'acquisition, de développement ou de refonte d'un système d'information et de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels. Le comité se basera sur le guide d'évaluation des facteurs relatifs à la vie privée de la Commission d'accès à l'information. Le comité doit aussi être consulté sur les mesures particulières à respecter en matière de protection des renseignements personnels pour les sondages et la vidéosurveillance.

De plus, le comité a la responsabilité de proposer au comité de direction des modifications à apporter au schéma de classification et s'il y a lieu, au calendrier de conservation, en lien avec la politique de gestion documentaire.

Présidé par le directeur général ou la personne qu'il désigne, ce comité est pluridisciplinaire afin de s'assurer de prendre en considération tous les aspects de la protection des renseignements personnels et la sécurité de l'information. Il est composé entre autres des personnes suivantes :

- Responsable de l'accès aux documents (directeur de l'administration);
- Responsable de la protection des renseignements personnels (directeur de l'administration);
- Responsable de la sécurité de l'information (directeur des technologies de l'information);
- Responsable de la gestion documentaire (directeur des technologies de l'information et adjointe à la direction générale);
- Toute autre personne dont l'expertise est requise.

7.3 Gestionnaire d'un service qui détient les actifs informationnels

Le gestionnaire d'un service qui détient les actifs informationnels doit faire en sorte que la protection des renseignements personnels et la sécurité de l'information soient une préoccupation constante pour son personnel. Il doit sensibiliser les employés à l'importance des enjeux concernant l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information et les informer sur ces sujets. Il doit également s'assurer que les moyens de sécurité sont employés de façon à protéger l'information que son personnel utilise. Il est le premier responsable de la sécurité et doit voir à ce que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement.

7.4 Responsable de l'accès aux documents et de la protection des renseignements personnels

Il incombe au responsable de l'accès aux documents et de la protection des renseignements personnels d'aider le personnel à mieux circonscrire l'interprétation et l'administration de la Loi sur l'accès lors de toute situation impliquant la cueillette, la communication, la conservation et la destruction de renseignements confidentiels ou personnels. Les déclarations de fichiers de renseignements personnels sont réunies dans un répertoire.

7.5 Responsable de la sécurité de l'information

La principale tâche du responsable de la sécurité de l'information est d'assister le directeur général dans l'établissement d'un processus de gestion intégrée et d'amélioration continue de la sécurité de l'information détenue par l'Office. Le responsable de la sécurité de l'information se réserve le droit d'intervenir, au nom de l'Office, lorsqu'il juge que la sécurité des actifs informationnels où la protection des renseignements personnels est menacée.

De plus, il assiste les gestionnaires et les détenteurs en leur fournissant des moyens techniques de sécurité, comme un contrôle d'accès, un plan de sauvegarde, un plan de secours, un antivirus, etc. Il s'assure de la conformité de ces moyens technologiques avec les besoins de l'Office en matière de protection des renseignements personnels et de la sécurité de l'information. Il veille également à ce que le développement du système informatique soit adapté à l'accès à l'information, à la protection des renseignements personnels et à la sécurité de l'information. Il fournit les moyens et les mécanismes de sécurité permettant d'assurer la protection des actifs informationnels et la continuité des services, en plus de voir à ce que la sécurité de l'information soit intégrée dans le développement des systèmes informatiques.

7.6 Responsable de la gestion documentaire

Le responsable de la gestion documentaire est consulté pour la conception des systèmes de l'Office et s'assure que les documents auront, à toutes les étapes de leur cycle de vie, les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois. Le responsable de la gestion documentaire collabore étroitement avec le responsable de la sécurité des informations. Il prépare aussi un calendrier de conservation des documents.

7.7 Direction des ressources humaines

La Direction des ressources humaines s'assure que tous les nouveaux employés de l'Office possèdent l'information leur permettant d'assumer leurs responsabilités en matière d'accès à l'information, de protection des renseignements personnels et de sécurité de l'information.

7.8 Utilisateurs

Les responsabilités des utilisateurs consistent à appliquer et à respecter la présente politique. Ils sont également tenus d'utiliser les moyens de sécurité et s'assurer de la protection des renseignements personnels selon les modalités établies par le comité. L'utilisateur est responsable de protéger l'accès et la confidentialité de tous les renseignements confidentiels qu'il détient ou utilise. Il ne doit accéder ou utiliser des renseignements confidentiels dont il n'a pas la responsabilité dans le cadre de ses fonctions.

Les utilisateurs se doivent d'aviser leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité des actifs informationnels et des renseignements détenus par l'Office.

Tout utilisateur des systèmes de l'Office a l'obligation de signaler à leur gestionnaire tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité, tel que le vol, l'intrusion dans un réseau ou un système, des dommages délibérés, l'utilisation abusive ou malveillante, la fraude, les actions contraires à l'éthique, etc.

7.9 Communication à des fins d'étude, de recherche ou de production de statistiques; communication à un organisme gouvernemental; communication à l'extérieur du Québec; communication dans un processus de deuil

Le responsable de l'accès à l'information et de la protection des renseignements personnels doit s'assurer de la conformité, selon la loi en vigueur, des documents transmis à des fins d'étude, de recherche ou de production de statistiques, lors de communication avec des organismes gouvernementaux, lors de communication à l'extérieur du Québec et lors de communication pour aider un conjoint ou un proche parent dans son processus de deuil. Il doit donner son accord avant la transmission de tout document qui sera fourni par l'Office.

8. Rôles et responsabilités en cas d'incident de confidentialité

Un incident de confidentialité peut survenir de différentes façons : transmission d'informations par erreur, perte de données, vol de données, fuite ou diffusion de données. L'incident peut se faire avec des documents physiques ou numériques.

Selon la nature de l'incident de confidentialité, le responsable diffère, mais le directeur de l'administration doit être informé en tout temps.

- Lors d'un incident lié à un document physique (papier) ou à un support numérique de type clé USB qui contient des informations confidentielles, le gestionnaire du service responsable de l'information prend en charge l'événement.
- Lorsque l'incident est lié à une erreur de transmission qui contient des renseignements personnels et confidentiels (mauvais destinataire, données non liées au dossier requis, données transmises en trop, etc.), le directeur de l'administration prend en charge l'événement.
- Pour les incidents liés aux données numériques (vol, perte, fuite), le directeur des technologies de l'information et le directeur de l'administration prennent en charge l'événement. Une cellule de crise est mise en place pour fins de décision.

La personne qui devient responsable de l'événement, doit déterminer la gravité de l'incident en complétant la grille d'analyse, voir « Annexe 3 » et il en remet une copie au directeur du service de l'administration.

Dans tous les cas, la direction générale sera informée de l'incident et une cellule de crise pourrait être requise. La cellule de crise est composée du comité de direction, incluant la conseillère en communications dans le but d'informer les parties prenantes tel que prévu à l'article *63.8 de la Loi*. La cellule de crise est liée par la confidentialité des discussions. La cellule de crise peut s'adjoindre procureurs, professionnels en sécurité de l'information et toute autre ressource pertinente.

Si la cellule de crise détermine qu'il y a un risque qu'un préjudice sérieux soit causé, le directeur de l'administration doit communiquer avec la Commission d'accès à l'information en complétant le formulaire d'avis et en l'acheminant par écrit à la commission. De plus, le directeur général avisera le (la) président (e) du conseil d'administration.

9. Droit des utilisateurs

Les utilisateurs des services de l'Office ont le droit de demander l'accès, la rectification ou la suppression de leurs renseignements personnels détenus par l'Office. Pour exercer ce droit, ils doivent contacter le Responsable de l'accès aux documents et de la protection des renseignements personnels aux coordonnées fournies sur notre site internet.

10. Droit à la portabilité

Le droit à la portabilité permet à toute personne d'obtenir la communication, dans un format technologique structuré et couramment utilisé, des renseignements personnels informatisés qu'elle a fournis à un organisme public, par exemple lors d'une prestation électronique de services. Une personne peut demander l'accès à ses renseignements personnels pour son

propre usage dans le but, notamment, de conserver ces derniers sur un espace de stockage privé ou encore de les communiquer à un tiers de son choix.

11. Reddition de compte

Annuellement, le comité dépose un rapport au conseil d'administration sur les mesures prises par l'Office en matière de protection des renseignements personnels.

12. Entrée en vigueur et approbation

La présente politique entre en vigueur sur approbation du conseil d'administration de l'Office.

Nº résolution : OM-2023-246.4.3

Adopté par le conseil d'administration le 21 septembre 2022.

AUTORISATION DE COMMUNIQUER DES RENSEIGNEMENTS

IDENTIFICATION DU REQUÉRANT / LOCATAIRE

NOM	PRÉNOM
DATE DE NAISSANCE	**N° DE DOSSIER**

IDENTIFICATION DU REPRÉSENTANT DU REQUÉRANT / LOCATAIRE

NOM	ORGANISME	TÉLÉPHONE
NOM	**ORGANISME**	**TÉLÉPHONE**
NOM	**ORGANISME**	**TÉLÉPHONE**

J'autorise l'Office municipal d'habitation de Québec (OMHQ) et les représentants désignés aux présentes à échanger les renseignements personnels pertinents à l'évaluation de mes besoins d'aide en vue de l'analyse de mon admissibilité en vertu de l'article 14.2 du Règlement sur l'attribution d'un logement à loyer modique et/ou de mon maintien en logement en vertu de la Partie 2 du bail et du règlement d'immeuble. J'autorise la cueillette des renseignements suivants :

- ☐ **Renseignements personnels**
- ☐ **Renseignements de nature financière**
- ☐ **TOUS LES RENSEIGNEMENTS**
- ☐ **Plaintes au dossier**
- ☐ **Renseignements de nature médicale ou psychosocial**
- ☐ **Autres, Précisez** _____

À REMPLIR PAR LE REQUÉRANT / LOCATAIRE

SIGNATURE DU DEMANDEUR	DATE
X	

À COMPLÉTER PAR UN REPRÉSENTANT (MANDATAIRE) DU REQUÉRANT / LOCATAIRE

Si le document est signé par le représentant, le consentement est accordé au nom du requérant / locataire.

SIGNATURE DU REPRÉSENTANT	DATE
X	

Tout renseignement personnel que possède l'Office municipal d'habitation de Québec est protégé aux termes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. J'ai le droit de demander accès à ces renseignements, et je comprends qu'ils peuvent être utilisés ou divulgués dans les conditions prescrites par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

À moins qu'il ne soit annulé par le requérant ou par le locataire par l'envoi d'un avis écrit à l'Office municipal d'habitation de Québec, ce formulaire demeurera valide pour faire les vérifications de l'admissibilité d'une demande de logement et/ou au maintien dans les lieux.

OMHQ – SOMHAC
110, rue de Courcelette
Québec (Québec) G1N 4T4

1. Vie privée et utilisation des renseignements personnels détenus par l'Office

1.1 L'Office municipal d'habitation de Québec (l'Office) et le fournisseur sont chacun responsables du respect de leurs obligations respectives aux termes des lois en matière de protection des renseignements personnels. En ce qui concerne les renseignements personnels que l'Office a transférés ou rendus autrement accessibles au fournisseur, l'Office déclare, garantit et convient qu'il a le pouvoir ou a obtenu tous les consentements nécessaires de la part des personnes admissibles requises aux termes des lois en matière de protection de renseignements personnels. Ceci afin de permettre le transfert, la divulgation, le traitement, la copie, l'altération, le stockage, la suppression ou toute autre utilisation par le fournisseur aux fins de la prestation des services et aux fins établies dans le présent contrat, et ils prennent chacun un engagement en ce sens.

1.2 Le fournisseur mettra en œuvre toutes les mesures administratives, physiques, logiques, organisationnelles et technologiques standards de l'industrie pour sécuriser et protéger les renseignements personnels confiés par l'Office contre tout accès, transfert ou toute divulgation, destruction, perte ou altération non autorisés, illégaux ou accidentels.

2. Confidentialité

2.1 Chaque partie s'engage à ne pas divulguer à quiconque tout renseignement confidentiel, sauf selon ce qui est permis aux présentes dispositions.

2.2 Chaque partie peut divulguer les renseignements confidentiels de l'autre partie :

a) à ses employés, dirigeants, mandataires, sous-traitants, conseillers ou sociétés affiliées qui ont besoin de connaître ces renseignements pour exécuter les obligations de la partie aux termes du présent contrat. Chaque partie s'assurera que ses employés, dirigeants, représentants, sous-traitants ou conseillers auxquels elle divulgue les renseignements confidentiels de l'autre partie respectent les présentes dispositions.

b) selon ce qui est exigé en vertu d'une loi ou d'une ordonnance d'un tribunal compétent ou par toute autorité gouvernementale ou chargée de la réglementation, à la condition que, sauf si la Loi ou la réglementation l'interdit, elle avise l'autre partie avant de procéder à une telle divulgation.

c) à ses avocats, comptables et consultants, investisseurs éventuels, prêteurs ou acheteurs, à la condition que chacune de ces personnes soit liée par des obligations de confidentialité semblables à celles énoncées dans le présent contrat.

2.3 Ni l'une ni l'autre partie ne peut utiliser les renseignements confidentiels de l'autre partie à toute fin autre que l'exécution de ses obligations ou l'exercice de ses droits aux termes du présent contrat.

A l'usage de la direction concernée ou de la cellule de crise en cas d'un incident de confidentialité

Cette grille vous permet d'évaluer les risques de préjudices lorsqu'un incident de confidentialité se produit.

Notions importantes :

Renseignement personnel (« RP »)
Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Incident de sécurité
Incident affectant la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel d'un établissement, incluant ou non des renseignements personnels.

Lorsque des renseignements personnels sont touchés par l'incident, **il s'agit d'un incident de confidentialité.**

- Accès, utilisation ou communication non autorisée par la loi d'un RP
- Perte d'un RP
- Toute autre atteinte à la protection d'un RP

Renseignements sensibles
Renseignements qui, de par leur nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de leur utilisation ou communication, suscitent un haut degré d'attente raisonnable en matière de vie privée.

1. Date ou période de l'événement _____

2. Type d'incident / Cause de l'incident

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

3. Des renseignements personnels sont-ils visés ?

- ☐ 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.Inscrire l'incident au registre et continuer l'analyse pour évaluer les conséquences appréhendées et les mesures à prendre.

4. Quels renseignements sont visés ?

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

☐ **Renseignements génétiques ou biométriques**
Ex. : Empreintes digitales, signature vocale, ADN, etc.

☐ **Autre, Précisez** _____
Ex. : Antécédents judiciaires, dossier d'employé, etc.

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

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

5. Ont-ils été récupérés ou détruits ?

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

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

Précisez _____

7. Combien de personnes sont visées et quel est le groupe de personnes visées ? (employés actuels ou antérieurs, locataires actuels ou antérieurs, requérants) ?

Nombre de personnes visées : _____

Groupe de personnes visées : _____

8. Des conséquences peuvent-elles néanmoins être appréhendées ?

☐ Oui, continuez l'analyse.
☐ Non, vous devez inscrire l'incident au registre.

9. Quelles sont les conséquences appréhendées de l'utilisation du RP ?

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

10. Quelle est la probabilité de l'utilisation du RP à des fins préjudiciables ?

- ☐ Faible
- ☐ Moyen
- ☐ Élevé

11. 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 à compléter par le directeur de l'administration)
- ☐ 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.

_____
Nom de la personne ayant fait l'évaluation

_____ _____
Signature de la personne ayant fait l'évaluation **Date**

_____
Nom du responsable de l'accès à l'information

_____ _____
Signature du responsable de l'accès à l'information **Date**