CHAMBRE DE L'ASSURANCE DE DOMMAGES	POLITIQUE	
	DATE DE LA RÉSOLUTION ET DE L'ENTRÉE EN VIGUEUR : **2013-12-10**	DERNIÈRE MISE À JOUR : **2013-12-10**
	APPROUVÉ PAR : **Conseil d'administration**	DATE D'ABROGATION : **AAAA-MM-JJ**

Politique de sécurité des renseignements personnels et confidentiels de la Chambre de l'assurance de dommages

1. Introduction

En vertu de l'article 286 de la *Loi sur la distribution de produits et services financiers*, la ChAD est soumise à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. La Chambre a la responsabilité d'assurer la confidentialité de certains renseignements et doit prendre les mesures de sécurité qui s'imposent pour ce faire.

2. Objet de la politique

Cette politique vise à protéger les renseignements personnels et confidentiels que gère la ChAD.

3. Application

Cette politique s'applique à tous les employés de la Chambre, aux administrateurs, aux membres de comités ainsi qu'aux différents consultants informatiques ou autres fournisseurs de services. Elle s'applique pendant toute la durée de leur lien d'emploi ou d'affaires et même après la fin d'emploi ou la fin de la relation d'affaires.

4. Définitions

Renseignement personnel : renseignement qui concerne une personne physique et qui permet de l'identifier. Ces renseignements peuvent être identitaires (ex : nom, adresse, numéro de téléphone), financiers (ex : numéro de carte de crédit), médicaux, liés aux activités professionnelles (ex : dossier d'employé), etc.

Renseignement confidentiel : voici une liste non exhaustive de renseignements confidentiels détenus par la Chambre :

- renseignement, concernant un individu ou une entreprise, obtenu dans le cadre d'une enquête menée par le bureau du syndic;
- renseignement, concernant un individu ou une entreprise, obtenu dans le cadre d'une inspection menée par le service d'inspection;
- renseignement, concernant un individu ou une entreprise, obtenu dans le cadre de la gestion de la formation continue obligatoire;
- renseignement, concernant un individu ou une entreprise, obtenu lors du processus disciplinaire.

Mot de passe : code unique et confidentiel qui, pour être sécuritaire, doit être composé d'au moins huit caractères incluant des chiffres et des lettres.

Nom d'utilisateur (*login* ou *username* en anglais) : Identifiant personnel permettant l'accès à un système informatique ou à une application.

Support : les renseignements peuvent exister sur différents supports (ex : dossier papier, ordinateur, téléphone intelligent) et sous différentes formes (ex : écrite, sonore, visuelle, informatisée).

Fournisseur de services : certains fournisseurs de services de la ChAD peuvent avoir accès à des renseignements personnels ou confidentiels, tel que les procureurs externes, le service de traitement de la paie, les firmes de sondage, les entreprises de publipostage ou les imprimeurs. Aux fins de la présente politique, les administrateurs et les membres des différents comités de la ChAD sont considérés comme des fournisseurs de services.

5. Collecte

Seuls les renseignements personnels et confidentiels nécessaires à la réalisation des différentes fonctions de la Chambre peuvent être colligés par les employés ou les fournisseurs de services.

6. Accès

Les employés et les fournisseurs de services peuvent avoir accès aux renseignements personnels et confidentiels détenus par la Chambre, mais doivent se limiter uniquement aux renseignements qui leur sont nécessaires dans l'exercice de leurs fonctions.

7. Conservation

La Chambre peut conserver à ses dossiers les renseignements personnels et confidentiels aussi longtemps qu'il le faut pour les fins auxquels ils sont dédiés. Le Plan de classification des documents de la ChAD précise les différentes règles de conservation des documents.

8. Mesures de sécurité

Afin de protéger les informations personnelles et confidentielles en sa possession, la Chambre a adopté diverses mesures de sécurité, notamment :

- À l'extérieur des heures de travail, les locaux de la Chambre sont accessibles via une carte d'accès;
- Tout classeur contenant des renseignements personnels et confidentiels est verrouillé et son accès limité aux employés ayant besoin de l'information dans l'exercice de leurs fonctions;
- Tout fichier informatique contenant des renseignements personnels et confidentiels est accessible par nom d'utilisateur et mot de passe, et ce, suivant certains droits prédéfinis;
- Les mots de passe doivent être modifiés minimalement à tous les six mois;
- Les serveurs sont installés dans un local verrouillé;
- Une copie de sauvegarde des serveurs et une copie-miroir des serveurs sont conservées à l'extérieur des bureaux de la Chambre.
- Le réseau de la Chambre est protégé par des systèmes de pare-feu, d'antivirus et de détection d'intrusion, lesquels sont revus sur une base continue afin de garantir la sécurité et la confidentialité des renseignements.

- Les connexions à distance (Extranet, Intranet et d'administration des systèmes) sont protégées par nom d'utilisateur et mot de passe. L'Intranet doit être accessible uniquement par connexion VPN (Virtual Private Network).
- L'accès aux téléphones cellulaires et tablettes doit également être protégé par mot de passe et muni d'un système de verrouillage automatique après quelques minutes d'inutilisation.

9. Télétravail

Lorsque les renseignements personnels ou confidentiels sont accessibles aux employés à l'extérieur des bureaux de la Chambre, l'accès doit être contrôlé par un nom d'utilisateur et un mot de passe.
Si des renseignements personnels ou confidentiels sont sauvegardés sur des portables ou des ordinateurs personnels, l'accès doit être restreint dans le temps aux seuls moments où ces renseignements sont nécessaires. Par la suite, les renseignements doivent être détruits de façon sécuritaire après leur utilisation. Tous les portables de la Chambre sont munis de système de pare-feu et d'antivirus. Les ordinateurs personnels utilisés pour le travail doivent également l'être.

Les clés USB qui contiennent des renseignements personnels ou confidentiels doivent également être encryptées et protégées par des mots de passe. Ces renseignements doivent obligatoirement être supprimés de façon sécuritaire lorsque leur utilisation n'est plus requise.

Pour assurer une plus grande sécurité, un mécanisme de verrouillage automatique doit être installé sur les ordinateurs, les tablettes et les téléphones intelligents.

Lors de l'utilisation de réseau sans fil (WiFi), pour se connecter à distance au réseau de la ChAD, l'employé doit s'assurer que le réseau sans fil est protégé. Si l'employé doit utiliser un réseau sans fil public, il ne doit pas se connecter au réseau de la Chambre.

10. Suite à un départ d'employé

Lors du départ d'un employé, la Chambre:

- désactive l'accès de l'employé à son compte de courriel;
- redirige temporairement l'adresse courriel de l'ex-employé afin de recevoir les courriels, aviser les correspondants du départ de l'employé et les traiter;
- désactive l'accès local et à distance au réseau de la Chambre;
- désactive la carte d'accès au bureau de la Chambre;
- désactive le téléphone cellulaire et la boîte vocale du poste téléphonique;
- récupère, s'il y a lieu, le portable, les dossiers et tout autre appareil comportant des renseignements personnels ou confidentiels.

11. Fournisseurs de services

Les renseignements personnels peuvent être communiqués à des fournisseurs de services de la Chambre. Dans de telles circonstances, la Chambre exige qu'ils n'utilisent pas ces informations à d'autres fins que celles de lui fournir le service en question. Ces fournisseurs de services doivent également s'engager à prendre toutes les mesures nécessaires pour protéger les renseignements personnels et confidentiels portés à leur connaissance durant la période de prestation des services. Ces engagements sont valides tant pendant qu'après la période de prestation des services.

12. Destruction des documents

Lorsque la Chambre estime qu'elle n'a plus besoin des renseignements personnels et confidentiels aux fins pour lesquelles ils ont été recueillis, elle les détruit de façon sécuritaire, par déchiquetage, dans les bureaux de la Chambre ou via un fournisseur externe qui déchiquette et récupère des boîtes scellées conçues à cette fin.

13. Responsable de l'application de la politique

Le comité de gestion doit veiller à ce que cette politique soit connue et respectée par les employés de la Chambre. La présente politique est, entre autres, fournie à tous les nouveaux employés de la Chambre dans les premiers jours de leur embauche.

14. Diffusion de la politique et engagement

Les employés de la Chambre ont pris connaissance de la présente politique et doivent s'engager à s'y conformer et de ce fait à respecter le caractère confidentiel des renseignements.

Tel que prévu par le Code d'éthique et de déontologie, l'employé signe un engagement à respecter la confidentialité des informations. Tout employé qui ne respecte pas ses obligations en matière de protection des renseignements personnels et confidentiels s'expose à des mesures disciplinaires.

Advenant un départ d'employé, celui-ci est tenu de respecter cet engagement de confidentialité. Tout ancien employé qui ne respecte pas ses obligations en matière de protection des renseignements s'expose à des poursuites civiles.

Tel que prévu par leur code d'éthique et de déontologie, les administrateurs de la CHAD ainsi que les membres de comités signent un engagement à respecter la confidentialité des informations.

Dans les contrats conclus avec les différents fournisseurs de services, un engagement à respecter la confidentialité des informations doit être prévu.

15. Entrée en vigueur

Cette politique, approuvée par le conseil d'administration de la Chambre, entre en vigueur le 10 décembre 2013.

ANNEXE 1

Engagement des employés à respecter la Politique de sécurité des renseignements personnels et confidentiels de la Chambre de l'assurance de dommages

Je _____ *(nom)*, employé de la ChAD, reconnais avoir reçu copie de la *Politique de sécurité des renseignements personnels et confidentiels de la ChAD*. Je reconnais l'avoir lue et en comprendre le sens et la portée.

Je m'engage à respecter les principes de sécurité concernant les renseignements personnels et confidentiels énoncés dans la politique.

J'AI SIGNÉ À _____, le_____

_____