



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte à la vie privée

Mon engagement

Afin de vous donner accès aux produits et aux services financiers, je recueille certains de vos renseignements personnels et assure la protection de ceux-ci. Je respecte la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), une loi fédérale concernant la protection des renseignements personnels, et toute loi provinciale qui s'applique. Je base également cette politique sur les recommandations et sur le code déontologique de la Chambre de la sécurité financière qui est l'organisme d'autoréglementation de notre industrie. Voyez en annexe B les références au code déontologique, ainsi que les questions fréquemment posées.

Responsabilité

Je suis responsable des renseignements personnels que je reçois de mes clients. Je protégerai ces renseignements, quel que soit le moyen utilisé lors de la transmission.

Consentement

Je recueillerai uniquement les renseignements avec votre consentement. Il y aura utilisation vos renseignements personnels pour trouver des produits, des concepts et des services financiers qui répondent aux besoins que vous avez identifiés. En signant le formulaire d'autorisation, vous consentez, en votre nom ainsi qu'au nom de vos liquidateurs, administrateurs ou cessionnaires, à :

- Fournir des renseignements exacts tout au long de notre relation d'affaires et au fur et à mesure que votre situation évolue.
- Me permettre d'utiliser, de transmettre et de divulguer ces renseignements au besoin à mes fournisseurs, associés et agents généraux administrateurs, qui pourraient conserver certains renseignements dans leurs dossiers pour une utilisation et une recommandation ultérieure par moi, mes fournisseurs et tout cessionnaire.
- Me permettre de conserver vos renseignements personnels, y compris les renseignements médicaux qui apparaissent sur vos propositions, dans mes dossiers papier et électroniques aussi longtemps que vous souhaitez faire affaires avec moi ou que je doive satisfaire à un besoin commercial ou réglementaire en conservant les renseignements.
- Céder votre dossier, y compris vos renseignements personnels, à un autre agent et/ou AGA, pour continuer à répondre à vos besoins, advenant l'invalidité, le décès, la retraite ou tout autre événement majeur mon cabinet. Vous avez cependant le droit de choisir votre propre agent à ce moment-là, si jamais vous n'êtes pas d'accord avec celui qui vous a été attribué.

Raisons de la collecte / utilisation / conservation

Je recueille tous les renseignements personnels (y compris les renseignements médicaux et financiers ainsi que ceux sur la société et les renseignements qui y sont liés) avec votre consentement. Je les utilise et les conserve uniquement afin de fournir des conseils, d'administrer des produits ou des services que vous achetez par mon entremise et de vous conseiller de nouveaux produits ou services qui pourraient vous intéresser.

Limite de la collecte

Je recueille et conserve uniquement les renseignements qui m'aident à vous conseiller, y compris les renseignements personnels, financiers et médicaux, et à répondre à mes obligations réglementaires. J'utilise uniquement des moyens équitables et légaux pour recueillir ces renseignements.

Limite de l'utilisation / communication / conservation

J'utiliserai et divulguerai vos renseignements personnels afin de remplir mes fonctions, de vous conseiller et, s'il y a lieu, de respecter la loi. Les renseignements personnels contenus dans votre dossier client seront communiqués seulement :

- À mes employés et aux personnes que j'aurai autorisé, comme par exemple des professionnels afin de vous aider dans des domaines d'expertise qui dépassent ma compétence.



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

- Aux compagnies dont j'offre les produits et les services et à leurs employés et mandataires pour leurs activités visant à vous fournir ou à chercher à vous fournir des produits et des services financiers, ou pour toute autre activité connexe (et en lien avec toute autre fin que vous avez autorisée);
- Aux tiers fournisseurs de services sélectionnés que j'aurai autorisé; s'ils sont situés à l'étranger, vos renseignements personnels peuvent alors être assujettis aux lois applicables, y compris les lois sur l'accès à l'information des autorités publiques, d'autres pays;
- Aux personnes ou aux entités à qui vous y avez donné accès ou qui sont autorisées à y accéder en vertu de la loi.

J'ai l'obligation de conserver la plupart des renseignements que je recueille pour des raisons réglementaires, y compris l'exigence de démontrer que les recommandations que je fais sont appropriées et répondent à vos besoins identifiés.

Conformément aux lois applicables et à votre autorisation écrite, vous avez le droit de prendre connaissance des renseignements personnels qui sont contenus dans votre dossier. À votre demande, des copies (et non des originaux) d'autres documents personnels, comme des polices d'assurance, des testaments ou des mandats (procurations), peuvent être conservées dans votre dossier.

Exactitude des renseignements

Afin de faire les recommandations appropriées, je dois recevoir des renseignements exacts. Il m'incombe de conserver les renseignements à votre sujet aussi exacts et à jour que possible. Si la situation le permet, je tenterai de mettre à jour vos renseignements personnels afin de déterminer si les recommandations que j'ai faites sont toujours appropriées selon l'évolution de votre situation. Cependant, je me fie également à vous pour me fournir des mises à jour régulières pour la même raison. Vous pouvez passer en revue les renseignements personnels que je conserve à votre sujet sur demande.

Efforts déployés afin de protéger vos renseignements personnels

Tous les membres du personnel, les conseillers associés, les agents généraux administrateurs et les fournisseurs qui ont accès aux dossiers des clients doivent protéger ces renseignements, les garder confidentiels et les utiliser uniquement aux fins prévues. Les renseignements qui ne sont plus requis aux fins prévues seront détruits. J'ai également mis en place des mesures de protection physiques et informatiques, ainsi que d'autres processus, pour protéger les renseignements des clients d'un accès non autorisé.

En annexe A, vous trouverez notre procédure en cas de manquement / brèche / atteinte à la protection de vos renseignements personnels.

Vos choix en matière de renseignements personnels

Vous pouvez retirer votre consentement en tout temps (sous réserve de restrictions contractuelles ou légales de me fournir un préavis raisonnable) en communiquant avec moi. Si vous retirez votre consentement, je pourrais être dans l'impossibilité de vous fournir les produits ou les services demandés et je pourrais devoir mettre fin à notre relation d'affaires.

Votre droit de porter plainte

Si vous avez des préoccupations concernant la collecte, l'utilisation ou la divulgation de vos renseignements personnels, vous avez le droit de porter plainte auprès de moi ou du Commissariat à la protection de la vie privée :

Chef de la protection des renseignements personnels :

Cabinet de services financiers Huard & associés
Jennie Huard
326, rue Lortie, Donnacona, Québec G3M 0B9
418 552-0135 / jennie@cabinetha.com

Commissariat à la protection de la vie privée du Canada
30, rue Victoria, Gatineau, Québec K1A 1H3
Sans frais : 1-800-282-1376



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

ANNEXE A – Procédure en cas de manquement / brèche / atteinte

Une atteinte à la protection des renseignements personnels survient lorsqu'il y a accès non autorisé à des renseignements personnels ou collecte, utilisation ou communication non autorisée de tels renseignements. Ces activités sont « non autorisées » lorsqu'elles contreviennent aux lois applicables en matière de protection des renseignements personnels, telles que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), ou aux lois provinciales similaires en matière de protection des renseignements personnels. Certaines des atteintes les plus courantes à la protection des renseignements personnels surviennent lorsque les renseignements personnels d'un consommateur, d'un patient, d'un client, ou d'un employé sont volés, perdus ou distribués par erreur (p. ex., le vol d'un ordinateur contenant des renseignements personnels ou l'envoi par erreur d'un courriel contenant des renseignements personnels à la mauvaise personne). Une atteinte peut également être la conséquence d'une procédure déficiente ou d'une défaillance opérationnelle.

Tel que déterminé par la Commission d'accès à l'information du Québec (www.cai.gouv.qc.ca), je suivrai les six (6) étapes suivantes en cas d'atteinte à la protection de vos renseignements personnels :

- 1) Évaluation préliminaire de la situation
- 2) Limite de l'atteinte à la vie privée
- 3) Évaluation des risques associés à l'atteinte
- 4) Notification à l'intention des personnes concernées
- 5) Prévention
- 6) Suivi

Étape 1 : Évaluation préliminaire de la situation

- a) Définir sommairement le contexte de la perte ou du vol de renseignements personnels :
 - Identifier les renseignements personnels touchés ainsi que leur support;
 - Identifier les personnes, leur nombre ainsi que le groupe de personnes (clients, employés, etc.) touchées;
 - Établir le contexte des événements (date, heure, lieu, etc.);
 - Identifier, si possible, les circonstances entourant la perte (cause, personnes susceptibles d'être impliquées dans l'incident, etc.);
 - Répertorier les mesures de sécurité physiques et informatiques en place lors de l'incident.
- b) Informer les autorités externes concernés qui doivent être avisés de l'incident immédiatement :
(avant l'évaluation des risques)
 - Service de police (si les circonstances laissent croire à la possibilité d'un crime);
 - Commission d'accès à l'information ([lien vers le formulaire](#))
- c) Désigner une personne ou une équipe responsable de la gestion de la situation.
- d) Informer les intervenants concernés à l'interne :
 - Dirigeants de l'organisme ou de l'entreprise;
 - Responsable de l'unité administrative concernée;
 - Responsable de la protection des renseignements personnels;
 - Conseiller juridique;
 - Direction des communications (gestion des médias et des appels de la clientèle).

Étape 2 : Limite de l'atteinte à la vie privée

Prendre sans tarder des mesures adéquates pour limiter les conséquences pour les personnes concernées d'une possibilité d'utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité :

- a) Prendre des mesures afin de limiter immédiatement les conséquences d'une perte ou d'un vol de renseignements personnels en s'assurant de mettre fin à la pratique non conforme le cas échéant;
- b) Récupérer les dossiers physiques ou numériques, selon le cas;



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

- c) Révoquer ou modifier les mots de passe ou les codes d'accès informatiques;
- d) Contrôler les lacunes dans les systèmes de sécurité.

Étape 3 : Évaluation des risques associés à l'atteinte

- a) Compléter une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels en cause, tenant compte de leur nature, leur quantité, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.;
- b) Déterminer le contexte de l'incident incluant :
 - la cause (ex. le caractère délibéré ou non de la perte ou du vol de renseignements personnels, l'erreur humaine, une faille informatique, etc.);
 - les auteurs connus ou probables des renseignements personnels perdus ou subtilisés (ex. organisation criminelle, public en général, etc.);
 - l'étendue de la situation (nombre de personnes touchées et secteurs touchés);
 - le caractère systémique ou non de la disparition des renseignements personnels (particulièrement lorsque la perte n'est pas générée directement par une intervention humaine);
 - une évaluation de la probabilité qu'un événement similaire se reproduise.
- c) Évaluer la possibilité que les renseignements personnels concernés fassent l'objet d'une utilisation préjudiciable pour les personnes concernées en tenant compte, notamment, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.);
- d) Évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels;
- e) Évaluer si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire;
- f) Déterminer les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels par des personnes malveillantes, notamment pour le vol d'identité;
- g) Déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.

Étape 4 : Notification à l'intention des personnes concernées

- a) Déterminer qui doit être mis au courant de la perte ou du vol de renseignements personnels en fonction de l'évaluation des risques :
 - Service de police : Dans les cas où la disparition peut résulter de la commission d'un crime, le service de police concerné doit être avisé des éléments entourant cette disparition tout d'abord et, ensuite, de toutes les démarches subséquentes. Il est nécessaire de porter une attention particulière afin de ne pas nuire à l'enquête et de préserver les éléments de preuve pouvant être pertinents;
 - Personnes concernées : Si la perte ou le vol de renseignements personnels présente un risque de préjudice pour les personnes concernées, celles-ci devraient en être avisées sans tarder. Il ne s'agit pas d'alarmer mais de prévenir afin de leur permettre de prendre les mesures pertinentes pour protéger leurs renseignements personnels;
 - Commission d'accès à l'information : Si les personnes concernées par les renseignements personnels proviennent du Québec, la Commission pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solution;
 - Autres : Il peut également être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc.

Toutefois, dans la diffusion des informations concernant la perte de renseignements personnels, une attention particulière doit être portée afin de ne pas aggraver le préjudice que pourraient subir les personnes concernées (ex. limiter au minimum les renseignements personnels dans les avis).

- b) Désigner les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone);
- c) Le cas échéant, identifier et consigner les motifs à l'origine de la décision de ne pas aviser les personnes concernées et les autres intervenants.

Avis aux personnes concernées par une perte ou un vol de leurs renseignements personnels :

Selon les circonstances, il pourrait s'avérer nécessaire d'aviser les personnes victimes de la perte ou du vol de leurs renseignements personnels. Cet avis pourrait inclure certains des éléments suivants:

- Le contexte de l'incident et le moment où il s'est produit ainsi qu'une description de la nature des renseignements personnels touchés ou potentiellement touchés, sans dévoiler de renseignements personnels spécifiques;
- Une description sommaire des mesures prises afin de limiter ou de prévenir tout préjudice, ainsi que la liste des personnes qui ont été informées de la situation (Service de police, Commission d'accès à l'information, etc.);
- Les actions prises par les organismes et les entreprises pour aider les personnes concernées (Service d'aide et d'information, Abonnement alerte crédit, etc.);
- Les mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice ou pour mieux se protéger (référence au document « Le vol d'identité » disponible à la Commission d'accès à l'information);
- Les autres documents d'information générale conçus pour aider les personnes à se prémunir contre le vol d'identité;
- Les coordonnées d'un interlocuteur de l'organisation qui peut répondre aux questions et à qui il est possible d'effectuer tout signalement;
- Les principales mesures qui seront prises pour éviter que la situation ne se reproduise (changement de pratique ou de processus, la formation du personnel, la révision ou l'élaboration de politiques, une vérification, un suivi périodique, etc.).

Étape 5 : Prévention

- a) Approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;
- b) Répertoire et examiner les normes, politiques ou directives internes en place au moment de l'incident, autant au niveau de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général;
- c) Vérifier si ces normes, politiques ou directives internes ont été suivies par les personnes impliquées, identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;
- d) S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;
- e) Évaluer la nécessité d'élaborer une politique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de l'organisme ou de l'entreprise;
- f) Formuler les recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;
- g) S'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés;
- h) Prévoir le suivi devant être accordé.

Étape 6 : Suivi

Il est important d'effectuer le suivi :

- a) du processus de traitement qui doit être appliqué lors d'une perte ou d'un vol de renseignements personnels et des résultats obtenus afin de l'améliorer, s'il y a lieu;
- b) des mesures de sécurité requises à la suite de l'incident et de leur performance afin d'améliorer les processus et place et de mettre à jour la Politique en matière de protection des renseignements personnels;
- c) de la communication de l'information pertinente à la Commission d'accès à l'information et au service de police impliqué, le cas échéant.

Tenue de dossier

Il est également obligatoire de tenir un registre de tous les événements d'atteinte à la protection des renseignements personnels, même si certains n'avaient aucun risque de préjudice grave. Tout événement doit être conservé au moins deux ans afin que le Commissariat à la protection de la vie privée puisse les examiner, sur demande.

Les dossiers doivent inclure, au minimum, les éléments suivants :

- la date ou durée estimée de l'atteinte ;
- une description des circonstances de l'atteinte ;
- la nature des renseignements en cause dans l'atteinte ;
- l'existence d'un rapport au Commissariat à la protection de la vie privée ou le nom des autres organisations avisées, s'il y a lieu ;



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte *(suite)*

- une courte explication des raisons pour lesquelles l'organisation a déterminé qu'il n'y avait aucun risque de préjudice grave si l'atteinte n'a pas fait l'objet d'un rapport au Commissariat à la protection de la vie privée.

Ressources

Vous trouverez des renseignements détaillés sur toutes vos obligations ayant trait à la protection des renseignements personnels au www.priv.gc.ca.



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

MESURES DE SÉCURITÉ IMPLANTÉES - informatiques et physiques

Antivirus avec Bit Defender GravityZone

Il s'agit de notre suite antivirus. L'antivirus analyse les applications et les fichiers qui pourraient être malveillants. C'est le 1er niveau de sécurité, la sécurité de base pour les ordinateurs. Bit Defender GravityZone possède certaines notions concernant les courriels entrants, les accès réseaux, il détecte des comportements louches de fichiers qu'il ne connaît pas. Sa protection est plus avancée que les protections standard des concurrents de l'industrie.

Payé à travers notre abonnement avec IT Cloud.

Pare-feu

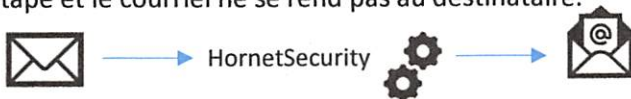
Nous utilisons Windows Defender et celui de Vidéotron, le fournisseur de services internet.

Chiffrement avec BitLocker

BitLocker est une spécification de protection des données développée par Microsoft, et qui fournit le chiffrement de partition. Lorsque l'on démarre un des ordinateurs, l'ordinateur nous demande une clé (code) Bit Locker. En cas de vol direct ou encore si une personne aurait accès aux documents à partir du disque dur de l'ordinateur, la personne a besoin de la clé pour accéder au contenu. Bloque à l'ouverture de l'ordinateur. Tous les fichiers sur l'ordinateur sont cryptés (chiffrés). Même en cas de bris, si notre technicien prend notre disque dur pour le mettre dans son système afin de récupérer nos informations, il aura besoin qu'on lui transmette la clé sinon cela ne fonctionnera pas.

Réception et envoi de courriels par HornetSecurity

La technologie de filtrage de HornetSecurity agit comme tiers/intermédiaire pour l'envoi et la réception des courriels. Si quelqu'un envoie un courriel, le courriel s'en va sur internet, passe par le filtre HornetSecurity et ensuite HornetSecurity filtre et analyse les logiciels malveillants / virus, filtre pour savoir s'il s'agit d'un courriel frauduleux ou spam et le livre à notre serveur de courriels. Et à l'inverse lorsqu'on envoie un courriel à partir de nos comptes Office 365, ça passe par le filtre d'HornetSecurity pour éviter qu'un attaquant envoie du spam ou des virus par nos envois de courriels – HornetSecurity l'intercepte à cette étape et le courriel ne se rend pas au destinataire.



Stockage de données avec SharePoint

Nous utilisons la suite Microsoft SharePoint qui sécurise l'information pour un accès extérieur à partir de nos adresses courriels. Nos adresses servent de clés de sécurité pour nos accès. Si une personne tente de se connecter à notre serveur SharePoint, elle a absolument besoin de notre adresse courriel et du mot de passe d'Office 365. SharePoint s'utilise en ligne sur les serveurs de Microsoft au Canada. Toutes les données sont encryptées et authentifiées.

Signature numérique des courriels

La signature numérique a également été mise en place (forme d'encryptage). Une signature numérique jointe à un message électronique est une autre couche de sécurité en protéger le destinataire d'un courriel que vous, et non un imposteur, n'avez pas signé le contenu du message électronique. Votre signature numérique, qui inclut votre certificat et votre clé publique, provient de votre ID numérique. Et cette identification numérique sert de marque numérique et signale au



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

destinataire que le contenu n'a pas été modifié lors du transit. Pour une meilleure compréhension, lorsqu'on envoie un courriel, une signature numérique est apposée sur chaque courriel. Lorsque le serveur courriel du destinataire reçoit le courriel, il détecte la signature numérique, il vérifie si la signature est valide. Si la signature est invalide, le courriel passe directement dans les indésirables. En cas d'usurpation d'identité, si le courriel n'est pas d'origine de notre serveur, il ira directement dans les spams. Le client ne verra pas passer le courriel potentiellement frauduleux. Lorsqu'on parle d'inclure une signature numérique, il est à noter qu'il ne s'agit pas d'une opération manuelle à laquelle nous procédons à chaque courriel, c'est une programmation qui le fait automatiquement chaque fois. Fait partie d'Office 365, serveur et gestion au Canada.

Signature électronique des documents avec DocuSign

DocuSign a été mis en place en juin 2021. Les fonctionnalités incluent notamment des services d'authentification, de gestion de l'identité des utilisateurs et d'automatisation des processus.

Les signatures électroniques et les documents sont encryptés puis traités par un algorithme de protection garantissant que la transaction numérique n'a pas été falsifiée ou compromise.

Avec la plateforme DocuSign, les signataires reçoivent, par courriel, un document à signer électroniquement. Chaque partie doit alors accepter d'examiner, de compléter et de signer le document. Les signatures électroniques peuvent être ajoutées à partir de la copie d'une signature manuscrite ou bien générées automatiquement par la plateforme DocuSign. Un niveau d'authentification additionnelle peut être proposé avec l'envoi d'un code par téléphone ou par vérification d'identité.

Le siège social est basé à San Francisco, aux États-Unis.

Site internet

Site sécurisé avec certificat SSL.

CGL Micro : Ils gèrent l'espace d'hébergement et les mises à jour critiques de Wordpress. Ils ont accès au cPanel et à Wordpress.

Gilles Larose : Effectue les corrections sur notre site Internet et gère notre nom de domaine chez WildWestDomains.

Nos fournisseurs :

CGL Micro (siège social)
199, rue Saint-Paul
Repentigny, Québec J5Z 2H9
450 654-4659

Maison Digilor inc.
Gilles Larose, pdg
1, chemin des Chouettes
Sainte-Anne-des-Lacs, Québec J0R 1B0
514 217-8876

WildWestDomains
2150 E Warner Road
Tempe, AZ 85284
Support : 480 624-2500
ARBN : 141 377 559
ABN : 53063126220

Sauvegarde (back up) avec Office 365 Back Up

Nous utilisons Office 365 Back Up. Tout ce qui est lié à Office 365 (courriels, One Drive, Teams, etc.) est sauvegardé 4 fois par jour (nuage). C'est sous forme d'abonnement, nos informations sont sauvegardées tant que l'on paye l'abonnement. Si l'on décide de cesser l'abonnement, nous pouvons faire une sauvegarde des fichiers et on les exporte sur notre périphérique choisi; ensuite on peut cesser l'abonnement.

<https://docs.microsoft.com/en-us/exchange/back-up-email>



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

Technicien informatique et services

À l'automne 2020, nous avons changé de fournisseur afin d'avoir un meilleur service, augmenter la sécurité et avoir un technicien proactif, qui comprend nos besoins. Notre personne-ressource est Nicolas Doré de TechniPC à Pont-Rouge. Il est également un des quatre propriétaires de TechniPC.

TechniPC Informatique inc. (service commercial)
44, rue du Collège
Pont-Rouge, Québec G3H 3A3

Chez TechniPC, les clients ne sont pas reliés ensemble, les clients sont gérés de façon indépendante. Le MFA est activé (authentification multifacteurs) est activé sur leurs plateformes. Est également activé, le Conditional Access (contrôle d'accès) pour limiter l'accès à différents pays.

Lorsque nous utilisons TeamViewer avec eux, il n'y a pas d'accès sauvegardé. À chaque connexion, nous devons leur transmettre le ID et mot de passe afin d'autoriser la connexion à distance. Avec TeamViewer, la connexion est sécurisée.

Nicolas Doré est administrateur délégué sur notre Office 365, ainsi que IT Cloud.

IT Cloud est un distributeur de services cloud pour les entreprises au Canada. Il est également un distributeur autorisé Microsoft.

<https://www.itcloud.ca/itcloud-ca/normes-et-securite/>

Nous avons plusieurs services et produits en abonnement avec IT Cloud :

- Licence Microsoft 365 Business Basic
- Spam & Malware Protection
- Office 365 Back Up / Total Protection
- Bitdefender Cloud Security
- Microsoft 365 Business Standard

IT Cloud Solutions
2525, rue Baillargeon
Trois-Rivières, Québec G8Z 2V4
877 374-0228

Mots de passe

Ils sont enregistrés sur One Drive, pas sur nos ordinateurs. Ils bénéficient donc des mêmes protections que pour les fichiers de client.

Téléchargements et installation de nouveaux logiciels

Tout est analysé par Bit Defender. L'ajout d'un compte utilisateur Admin sur chaque ordinateur sera implanté. Lorsque l'on voudra installer un nouveau logiciel, nous devons entrer le mot de passe du compte utilisateur Admin. Si un virus tente de s'installer il s'installera sur le compte Admin seulement, le compte sur lequel nous travaillons est protégé.

Formations pour reconnaître les courriels potentiellement dangereux, l'hameçonnage, le harponnage, etc.

Nous avons suivi 2 formations en ligne (par François Charron et Google) en plus de la lecture de documents mis en ligne par le Centre canadien pour la cybersécurité du gouvernement du Canada pour apprendre à mieux reconnaître les dangers du web et de son utilisation, ainsi que comment mieux protéger nos données.



Politique en matière de protection des renseignements personnels et procédure en cas d'atteinte (suite)

Mot de passe du réseau Wi-Fi

Le mot de passe est un mot de passe robuste avec lettres, chiffres et caractères spéciaux.

Mesures supplémentaires

Le bureau est muni d'un système d'alarme relié à une centrale.

Des caméras extérieures qui sont également reliées à la centrale et aux cellulaires des propriétaires de l'immeuble ont été ajoutées à l'été 2021.

L'accès au bureau est limité. Les portes sont barrées lorsque nous sommes absents.

Les classeurs sont tous barrés par des codes différents.

Signé à Donnacona, Québec, ce 26 e jour de avril 2023

Signature de la conseillère en sécurité financière (CSF), soit Mme Jennie Huard :