La prévention des sinistres, j'y vois !

Protégez votre entreprise contre les atteintes à la vie privée

METTEZ EN PLACE DES MESURES POUR UNE GESTION ADÉQUATE DES RENSEIGNEMENTS PERSONNELS

En tout temps et en tout lieu, les données confidentielles doivent être protégées, conservées de façon sécuritaire et limitées aux personnes autorisées.

- Veillez à ce que personne n'ait accès à votre ordinateur ni au contenu de vos dossiers sans autorisation. Placez l'équipement de bureau partagé, comme les télécopieurs, les photocopieurs, les boîtes à courrier individuelles ou communes et les casiers de traitement de documents, à des endroits non accessibles au public.
- Gardez sous clé dans des armoires, classeurs ou autres endroits à accès autorisé seulement les dossiers contenant des renseignements personnels sur des clients, des patients, des employés, des comptes, etc.
- Établissez des procédures écrites afin de déterminer qui peut consulter, modifier ou détruire des renseignements personnels. Configurez le réseau informatique afin que seules ces personnes puissent avoir accès à des répertoires ou dossiers particuliers.
- Limitez l'accès aux données confidentielles aux personnes appelées à les utiliser dans le cadre de leur travail et bloquez-en l'accès au personnel qui travaille en dehors des heures habituelles de bureau ainsi qu'au personnel d'entretien ou de sécurité.

Déterminez les renseignements essentiels à conserver

La protection des renseignements personnels nécessite une attention particulière. Conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et selon les lois provinciales, vous devez vous assurer que ces données demeurent confidentielles et sont conservées de façon sécuritaire.

- Recueillez et conservez uniquement les données qui sont essentielles pour l'entreprise.
- Mettez en place une politique de conservation des documents.
- Assurez-vous de détruire les renseignements désuets de manière sécuritaire.

Installez des systèmes de sécurité

Afin de déceler toute intrusion, procédez à l'ajout d'un système d'alarme anti-intrusion muni de dispositifs de détection périmétrique et volumétrique reliés à une centrale homologuée.

Exigez que tous les visiteurs signent un registre

Avant d'être autorisés à entrer dans vos bureaux, tous les visiteurs devraient signer un registre de visiteurs et montrer une pièce d'identité, qu'il s'agisse de fournisseurs, de clients ou d'employés potentiels.

intact ASSURANCE

03-M-181.1 (09-18)

Évaluez l'accès aux données aux entrepreneurs et fournisseurs

Déterminez les services nécessitant l'accès aux données confidentielles et assurez-vous que seuls les entrepreneurs et fournisseurs qui livrent ces services ont accès aux données. Par exemple, l'accès aux renseignements personnels sur les employés ne devrait être accordé que pour la rémunération et les avantages sociaux. Assurez-vous que les ententes avec les fournisseurs vous offrent une protection adéquate et que ces derniers :

- respectent les mesures de sécurité de votre entreprise;
- assument les frais et la correction de tout incident de mauvais usage ou de perte de données confidentielles;
- ont la capacité financière, par un cautionnement ou une assurance, de payer tous les frais de remédiation nécessaires en cas de perte de renseignements.

Effectuez des vérifications sur tous les employés

Instaurez des pratiques d'embauche pour tous les employés, en particulier pour ceux qui auront accès à des renseignements confidentiels. Ayez recours à des entreprises spécialisées dans la vérification des antécédents criminels et professionnels.

Établissez des lignes directrices en matière de protection des renseignements personnels

Tous les employés pouvant avoir accès à des renseignements confidentiels, y compris les employés d'entretien, les techniciens, les adjoints administratifs et les employés temporaires, devraient signer une entente de confidentialité et de sécurité.

Distribuez et expliquez à tous les employés les protocoles de protection des données (politique en matière de rangement de bureau, accès restreint aux données, lignes directrices pour les visiteurs, etc.). Passez en revue les pratiques sur une base régulière, au moins une fois par année. Redonnez une formation aux employés en cas de modifications apportées aux protocoles.

Mettez en place un programme d'audit

Instaurez des politiques sur les pratiques exemplaires et les normes de l'industrie. Effectuez des vérifications périodiques en vous assurant que :

a) les données confidentielles sont protégées lorsqu'elles ne sont pas utilisées;

b) seuls les utilisateurs autorisés ont accès aux renseignements confidentiels;

c) les registres de visiteurs sont bien tenus et les documents confidentiels sont détruits de manière appropriée.

Limitez l'usage de la technologie portable

Limitez le transfert des renseignements confidentiels des ordinateurs de bureau à des dispositifs portables comme des cellulaires, tablettes, ordinateurs portables, copies de sauvegarde, clés USB et disques durs amovibles. Si un transfert de données doit être fait sur ce genre de dispositifs, ceux-ci devraient être munis d'un logiciel de chiffrement avec un mot de passe fort. Ces renseignements doivent être supprimés des dispositifs portables dès qu'ils ne sont plus nécessaires ou qu'ils ont été transférés à d'autres dispositifs non portables pour conservation.

N'utilisez pas de réseaux sans fil non sécurisés

Les réseaux sans fil publics n'offrent pas de dispositifs de sécurité adéquats pour protéger les données confidentielles d'une entreprise. Assurez-vous que le réseau sans fil que vous utilisez offre une authentification et une communication sécurisées.

Assurez-vous que l'accès à distance à votre réseau est sécurisé

L'accès à distance à votre réseau devrait être fait par l'activation de connexions à un réseau privé virtuel (RPV). Tous les mots de passe par défaut pour accéder à votre réseau doivent être modifiés sur une base régulière.

Ayez recours à la protection par mot de passe et au chiffrement

Les renseignements confidentiels doivent toujours être chiffrés. Des technologies de chiffrement sont offertes à faible coût. Tous les usagers du système devraient recevoir un nom d'utilisateur unique et avoir un mot de passe fort qui doit être changé au moins une fois par trimestre. Effectuez un audit annuel des mots de passe.

Protégez-vous contre les logiciels malveillants

Afin de réduire les risques d'infections par un logiciel malveillant sur votre réseau :

1. Assurez-vous que votre réseau est protégé par un logiciel antivirus qui inclut un pare-feu.
2. Analysez régulièrement votre réseau pour détecter toute menace.
3. Restreignez l'accès à des sites jugés malveillants.
4. Ne cliquez jamais sur un lien et ne téléchargez jamais de fichiers provenant d'une source non fiable (courriel, site Web inconnu, etc.).

Mettez à jour tous vos systèmes et logiciels sur une base régulière

Pour assurer la meilleure protection informatique possible, téléchargez les plus récents correctifs de système et de sécurité et les mises à jour de tous vos logiciels et applications.

Détruisez le matériel informatique de manière appropriée

Instaurez des politiques pour la destruction adéquate des vieux ordinateurs, disques, bandes, photocopieurs, imprimantes, numériseurs, CD, clés USB et tout autre matériel pouvant contenir des renseignements confidentiels (des pratiques similaires devraient être adoptées pour la destruction adéquate des données confidentielles en format papier). Souvent, le matériel peut donner accès aux données, même si l'information a été supprimée. Ne vous fiez pas aux fonctions de « suppression » et de « corbeille » pour l'élimination des fichiers contenant des renseignements confidentiels. Il est toujours préférable de détruire le matériel et les dispositifs de mémoire dont on n'a plus besoin.

Appelez votre courtier, c'est votre meilleur conseiller.

VOUS VOULEZ EN SAVOIR DAVANTAGE SUR CE QUE VOUS POUVEZ FAIRE POUR PROTÉGER VOTRE ENTREPRISE ? VOTRE COURTIER D'ASSURANCE PEUT VOUS RENSEIGNER À CE SUJET.

https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/politiques-de-confidentialite/02_05_d_56_tips2/

https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/guide_org/