

Notre engagement à garder vos actifs en sécurité

CYBERSÉCURITÉ

Chez Patrimoine Richardson Limitée, nous reconnaissons que nous avons une responsabilité envers vous. En conséquence, nous voulons profiter de cette occasion pour vous rassurer sur les mesures de cybersécurité qui sont prises en tout temps pour protéger vos actifs.

Gestion des menaces

Patrimoine Richardson prend différentes mesures pour protéger ses systèmes contre la compromission des données, dont celles-ci :

- **Pare-feu de nouvelle génération** : Nous utilisons des pare-feu de nouvelle génération, qui inspectent les données qui traversent le pare-feu afin d'en vérifier la nature et de les classer de façon appropriée.
- **Sécurité des points d'accès améliorée** : Nos postes de travail sont tous équipés d'une protection évoluée contre les logiciels malveillants qui est mise à jour en temps réel, plusieurs fois par jour. Nous utilisons également une protection heuristique qui protège les postes de travail contre les menaces du jour zéro, avant même qu'elles ne soient détectées par la plupart des protections antivirus.
- **Gestion structurée des correctifs** : Les nouvelles menaces signalées dans les médias sont souvent des attaques qui profitent de vulnérabilités déjà connues et pour lesquelles des correctifs sont disponibles. Chez Patrimoine Richardson, nous observons un cycle de gestion des correctifs strict qui permet d'appliquer les correctifs sur nos serveurs et nos postes de travail bien avant la propagation du virus et ainsi de prévenir toute vulnérabilité.
- **Réseaux protégés** : Chez Patrimoine Richardson, nous avons séparé le WiFi de l'entreprise de la connexion WiFi des invités afin de permettre à ces derniers d'accéder aux ressources dont ils ont besoin, tout en bloquant l'accès au réseau de la société par des appareils ou des invités inconnus.

Analyse de la sécurité

Patrimoine Richardson recueille des données d'analyse dans ses principaux systèmes afin d'assurer un suivi des anomalies et de permettre à nos spécialistes de l'informatique de les examiner et de le corriger.

Protection de l'information et gestion de l'accès

- **Contrôle d'accès basé sur les rôles** : Comme Patrimoine Richardson utilise un grand nombre de systèmes, elle applique un contrôle



d'accès basé sur les rôles afin de s'assurer que l'accès aux données sensibles est réservé aux personnes dans des rôles bien précis et attribué selon le principe d'accès sélectif.

- **Sécurité des applications :** Les applications sont conçues au moyen d'une méthode d'authentification centralisée, ce qui nous permet de simplifier la sécurité et de faciliter la vérification de l'information grâce à un enregistrement chronologique des données amélioré.
- **Cryptage des appareils :** Patrimoine Richardson procède au cryptage de tous les ordinateurs portables afin d'éviter que les données soient compromises en cas de perte ou de vol d'un appareil.
- **Authentification unique:** Patrimoine Richardson utilise une solution d'authentification unique qui permet à nos employés de limiter le nombre de mots de passe. Cette pratique nous permet d'appliquer une politique de mot de passe rigoureuse.

Protection des applications et de l'infrastructure

- **Tests de pénétration :** Patrimoine Richardson embauche des pirates éthiques pour mettre à l'épreuve la robustesse de ses applications et de son infrastructure. Ces tests nous permettent de détecter tout changement dans notre infrastructure et ainsi de réduire le risque et d'augmenter la robustesse de nos systèmes.
- **Normes de développement des logiciels :** Patrimoine Richardson respecte les normes du secteur afin de s'assurer que tout logiciel développé à l'interne est sécuritaire. Un cycle de développement des systèmes (CDS) défini est respecté et Patrimoine Richardson adhère aux normes de l'Open Web Application Security Project (OWASP).
- **Centre de données sécurisé :** Patrimoine Richardson conserve toutes les données de production dans un centre de données ayant reçu les attestations SOC 1 et 2 (« System and Organization Control »). Du personnel est affecté au centre de données 24 heures sur 24, 7 jours sur 7, et le centre est équipé d'un système de sécurité et de surveillance vidéo et d'un contrôle d'accès anthropométrique.

- **Vérification de la sécurité physique des tiers :** Patrimoine Richardson mène des vérifications dans ses locaux afin de s'assurer que nos bureaux sont sécuritaires et que le personnel respecte la politique et protège l'information sensible des clients.
- **Gestion automatisée des correctifs :** Patrimoine Richardson a automatisé la gestion des correctifs afin de s'assurer que tous les correctifs de sécurité sont transmis à notre serveur et à notre plateforme de poste de travail, tout en limitant au minimum l'intervention du personnel des TI. De cette façon, l'exposition aux logiciels malveillants est considérablement réduite.

Gestion de la cybersécurité

- **Code de conduite :** Le code de conduite et l'éthique professionnelle de Patrimoine Richardson sensibilisent le personnel à l'importance de la cybersécurité.
- **Plan(s) de réaction aux incidents informatiques :** Patrimoine Richardson s'est dotée d'un plan de réaction aux incidents informatiques afin de pouvoir aviser rapidement les parties touchées en cas de compromission de données confidentielles.
- **Test du plan de continuité des activités :** Conformément à notre engagement à réduire au minimum les interruptions, Patrimoine Richardson a conclu une entente pour l'utilisation de locaux de tiers afin de pouvoir continuer d'assurer les activités commerciales névralgiques dans l'éventualité où les employés ne pourraient plus accéder à un ou plusieurs de nos bureaux ou en cas de panne de courant ou de perte de connectivité.

Nous apprécions la confiance que vous accordez à Patrimoine Richardson et nous prenons très au sérieux notre responsabilité de protéger vos actifs. Si vous avez des questions, n'hésitez pas à communiquer avec votre conseiller afin d'obtenir un complément d'information.

Notre force. Votre sécurité.

La robustesse du réseau de Patrimoine Richardson réside dans notre engagement envers une protection en profondeur. Ce principe garantit la mise en place de nombreuses protections afin qu'aucune vulnérabilité ou menace ponctuelle ne puisse compromettre le réseau.