**Politique de Cybersécurité de Sisley**

**Introduction :**

La cybersécurité est une priorité absolue chez Sisley pour protéger nos données sensibles, assurer la confidentialité de nos informations et maintenir la confiance de nos clients. Cette politique énonce les principes fondamentaux que chaque employé doit suivre pour garantir la sécurité de nos systèmes informatiques.

**Responsabilité de l'Utilisateur :**

* Chaque employé est responsable de la sécurité des informations auxquelles il a accès.
* Protégez vos identifiants, mots de passe et tout autre moyen d'authentification.

**Politique de Mots de Passe :**

* Les mots de passe doivent être robustes, uniques et changés régulièrement.
* N'utilisez jamais le même mot de passe pour plusieurs comptes.

**Accès aux Ressources Informatiques :**

* L'accès aux ressources informatiques est limité aux employés autorisés.
* L'utilisation de l'ordinateur professionnel à des fins personnelles est strictement interdite.

**Mises à Jour et Correctifs :**

* Assurez-vous que tous les logiciels, systèmes d'exploitation et applications sont régulièrement mis à jour avec les derniers correctifs de sécurité.

**Protection contre les Logiciels Malveillants :**

* Tous les employés doivent utiliser des logiciels antivirus approuvés et les maintenir à jour.
* Signalez immédiatement tout soupçon de logiciel malveillant à l'équipe informatique.

**Utilisation des Équipements Personnels :**

* L'utilisation d'équipements personnels sur le réseau de l'entreprise est soumise à des règles strictes et doit être approuvée par le département informatique.

**Accès Physique aux Locaux Informatiques :**

* L'accès aux locaux informatiques est restreint et contrôlé. Les employés doivent signaler toute personne non autorisée.

**Sensibilisation à la Cybersécurité :**

* Les employés participeront régulièrement à des programmes de sensibilisation à la cybersécurité pour rester informés des dernières menaces et des meilleures pratiques.

**Gestion des Incidents de Sécurité :**

* Toute violation de la sécurité doit être signalée immédiatement au département informatique.
* Des procédures d'investigation et de résolution seront mises en œuvre en cas d'incident.

**Réseaux Sociaux et Communications :**

* Soyez conscient des risques liés à l'utilisation des médias sociaux et des communications électroniques.
* Ne partagez pas d'informations sensibles en dehors des canaux sécurisés de l'entreprise.

**Notes Complémentaires :**

* La politique de cybersécurité est sujette à des révisions périodiques. Les employés doivent consulter les mises à jour régulièrement.
* Les formations sur la cybersécurité seront fournies régulièrement pour renforcer la compréhension des employés.

Nous comptons sur chaque employé pour jouer un rôle actif dans la préservation de la cybersécurité chez Sisley. En respectant ces directives, nous contribuons tous à créer un environnement informatique sûr et fiable.