RÈGLEMENT DE SÉCURITÉ INFORMATIQUE

Entreprise : [Nom de l'entreprise]
Responsable informatique : [Nom]
Version : [Date]

1. Objet du règlement

Ce règlement a pour but d'assurer la sécurité des systèmes informatiques, des données professionnelles et des communications numériques de l'entreprise. Il s'applique à l'ensemble du personnel ainsi qu'à toute personne ayant accès aux équipements ou aux services numériques de l'entreprise, notamment les collaborateurs fixes, temporaires, prestataires externes et partenaires techniques.

2. Utilisation des équipements informatiques

Les équipements informatiques mis à disposition (ordinateurs, téléphones, imprimantes, logiciels) doivent être utilisés exclusivement dans un cadre professionnel. Une utilisation personnelle est tolérée dans les limites du raisonnable, pour autant qu'elle ne porte pas atteinte à la sécurité des données ni à la productivité. L'installation de logiciels, l'ajout de périphériques ou toute modification de configuration doivent être validés par le service informatique. Toute utilisation de supports amovibles (clés USB, disques durs externes) nécessite une vérification antivirus préalable.

3. Accès, identifiants et mots de passe

Chaque collaborateur est personnellement responsable de la confidentialité et de la protection de ses identifiants. Les mots de passe doivent être suffisamment complexes, uniques pour chaque service utilisé, et renouvelés périodiquement. Il est interdit de partager ses accès, même temporairement. En cas de suspicion d'un accès non autorisé ou de compromission, l'utilisateur doit en informer immédiatement le service informatique.

4. Protection des données professionnelles

Les données sensibles, confidentielles ou à caractère personnel doivent être stockées uniquement sur les serveurs sécurisés de l'entreprise ou dans des solutions cloud agréées. Leur transmission à l'extérieur doit s'effectuer via des canaux protégés. Le stockage local non autorisé, ainsi que la copie sur des supports non sécurisés, est strictement interdit. Toute manipulation de données à caractère personnel doit se faire dans le respect de la législation en vigueur (LPD / RGPD).

5. Utilisation de la messagerie et d'internet

La messagerie professionnelle est un outil de travail. L'envoi d'e-mails à des fins privées doit rester exceptionnel et raisonnable. Il est formellement interdit d'utiliser la messagerie pour diffuser des contenus inappropriés, offensants ou non liés à l'activité professionnelle. Les pièces jointes et liens provenant d'expéditeurs inconnus doivent être traités avec prudence et signalés en cas de doute. La navigation sur internet doit se limiter à des sites en lien avec l'activité de l'entreprise. L'accès à des sites à risque, à contenu illicite ou non sécurisé est prohibé.

6. Télétravail et mobilité

Le télétravail impose les mêmes exigences de sécurité qu'au sein des locaux de l'entreprise. Les connexions doivent s'effectuer exclusivement via un VPN sécurisé. Les appareils utilisés à domicile doivent être protégés par un mot de passe et bénéficier d'une protection antivirus à jour. Le stockage local de données professionnelles est interdit, sauf autorisation préalable du responsable informatique. Le collaborateur reste responsable de l'environnement de travail à distance, notamment de l'accès non autorisé par des tiers.

7. Gestion des incidents de sécurité

Tout incident de sécurité, qu'il s'agisse d'un virus, d'un piratage, d'une perte ou d'un vol d'équipement, d'une tentative de fraude ou d'un comportement suspect, doit être immédiatement signalé au service informatique. L'entreprise dispose de procédures internes de réponse aux incidents, incluant la gestion des violations de données. Le non-respect des consignes de sécurité informatique peut entraîner des sanctions disciplinaires, voire des poursuites civiles ou pénales en cas de faute grave.

8. Engagement du collaborateur

Chaque collaborateur s’engage, par sa signature, à respecter l’ensemble des dispositions du présent règlement et à adopter un comportement responsable dans l’usage des outils numériques mis à sa disposition. Il reconnaît avoir été informé des règles applicables en matière de cybersécurité et des sanctions liées à leur non-respect.

Nom : .....
Fonction : .....
Date : .....
Signature : .....