Charte informatique pour la sécurité en télétravail

1. Introduction

Objectif de la charte

La présente charte a pour objectif de définir les règles et les bonnes pratiques en matière de sécurité informatique applicables au télétravail. Elle vise à protéger les actifs informationnels de l'entreprise contre les risques de cyberattaques, de pertes de données ou de tout autre incident pouvant compromettre l'intégrité, la confidentialité et la disponibilité des informations.

Portée

Cette charte s'applique à tous les employés de l'entreprise, ainsi qu'aux sous-traitants et partenaires, travaillant à distance sur des équipements informatiques, qu'ils soient fournis par l'entreprise ou personnels (BYOD).

2. Responsabilités des employés

Utilisation des équipements

Les employés doivent utiliser les équipements informatiques, qu'ils soient fournis par l'entreprise ou personnels, de manière responsable et sécuritaire. L'installation de logiciels non autorisés est interdite, tout comme l'usage de ces équipements à des fins non professionnelles pouvant compromettre la sécurité de l'entreprise.

Gestion des mots de passe

Les mots de passe utilisés pour accéder aux systèmes et applications de l'entreprise doivent être forts et uniques. Ils doivent être composés d'au moins 12 caractères, incluant des lettres majuscules et minuscules, des chiffres et des symboles. Le partage des mots de passe est strictement interdit.

Protection des données

Les données de l'entreprise doivent être stockées et partagées de manière sécurisée. L'utilisation de services de stockage en nuage non approuvés par l'entreprise est interdite. Les employés doivent également veiller à ne pas exposer les données sensibles à des tiers non autorisés.

3. Sécurité des connexions

Réseau Wi-Fi sécurisé

L'utilisation d'un réseau Wi-Fi personnel pour le travail à distance doit être sécurisée. Le réseau doit être protégé par un mot de passe fort et crypté via WPA2 ou WPA3. Il est recommandé de changer le nom par défaut du réseau Wi-Fi pour un nom non identifiable directement avec l'entreprise.

VPN

L'accès aux ressources internes de l'entreprise doit se faire via un VPN fourni et configuré par l'entreprise. Le VPN assure un tunnel sécurisé pour la transmission des données et doit être activé pour toute connexion à des services internes.

4. Sécurité des données

Chiffrement

Les données sensibles stockées sur les équipements des employés ou transmises via internet doivent être chiffrées. Cela inclut les disques durs, les clés USB et les communications par email ou via des applications de messagerie.

Sauvegarde des données

Les employés doivent effectuer régulièrement des sauvegardes des données critiques sur des supports sécurisés et approuvés par l'entreprise. Les procédures de sauvegarde doivent être définies et communiquées par le service informatique.

5. Gestion des incidents

Détection et rapport des incidents

Tout incident de sécurité, tel qu'une suspicion de malware, une perte de données ou un accès non autorisé, doit être immédiatement signalé au responsable de la sécurité informatique de l'entreprise. Une procédure claire de rapport doit être communiquée à tous les employés.

Réponse aux incidents

L'entreprise doit disposer d'un plan de réponse aux incidents de sécurité informatique, incluant la notification des autorités et des parties prenantes concernées, la cont
ainment des dommages et la récupération des systèmes et des données affectées.

6. Mise à jour des logiciels

Logiciels et systèmes d'exploitation

Tous les logiciels et systèmes d'exploitation utilisés dans le cadre du télétravail doivent être régulièrement mis à jour pour intégrer les derniers correctifs de sécurité. Les employés doivent activer les mises à jour automatiques lorsque cela est possible.

Antivirus et antimalware

L'utilisation d'une solution antivirus et antimalware à jour est obligatoire sur tous les équipements utilisés pour le télétravail. Les mises à jour doivent être appliquées dès leur disponibilité.

7. Formation et sensibilisation

Formations obligatoires

L'entreprise doit organiser des formations régulières sur la sécurité informatique à l'intention de tous les employés. Ces formations doivent couvrir les risques liés au télétravail, les bonnes pratiques à adopter et les procédures spécifiques à l'entreprise.

Bonnes pratiques et conseils

Le service informatique doit régulièrement communiquer des conseils de sécurité, des alertes sur les dernières menaces et des rappels des bonnes pratiques à suivre.

8. Surveillance et audit

Contrôles réguliers

Des contrôles de sécurité doivent être effectués régulièrement pour vérifier le respect de la charte de sécurité informatique. Ces contrôles peuvent inclure des audits de configuration, des tests de pénétration et des revues de procédures.

Audit de sécurité

Des audits de sécurité externes doivent être réalisés périodiquement pour évaluer l'efficacité des mesures de sécurité mises en place et identifier les éventuelles vulnérabilités.

9. Sanctions

Non-respect de la charte

Le non-respect des dispositions de cette charte peut entraîner des sanctions, allant de l'avertissement à des mesures disciplinaires, en fonction de la gravité de l'infraction.

10. Révision de la charte

Mise à jour

Cette charte sera révisée au moins une fois par an ou à chaque fois que des changements significatifs dans l'environnement de travail ou dans les technologies utilisées le nécessitent.

Conclusion

Engagement des employés
Chaque employé a un rôle crucial à jouer dans la protection de la sécurité informatique de l'entreprise. Par leur engagement et leur vigilance, ils contribuent à la sécurité de leurs propres données ainsi qu'à celle de l'entreprise dans son ensemble.

En suivant ces directives, l'entreprise vise à créer un environnement de travail sécurisé et à renforcer la confiance de ses clients et partenaires dans sa capacité à protéger les informations sensibles.