Quelles sont les obligations de cybersécurité du salarié en télétravail ?

Réponse courte

Le salarié en télétravail doit respecter l'ensemble des **règles de sécurité informatique** définies par l'employeur, conformément à la convention du 20 octobre 2020 et à la **charte informatique**. Ces obligations incluent l'utilisation exclusive du **matériel professionnel**, la connexion via un **VPN sécurisé**, le respect de la **politique de mots de passe**, le verrouillage des sessions et le signalement immédiat de tout **incident de sécurité**.

Le non-respect de ces obligations peut constituer une **faute disciplinaire** pouvant aller jusqu'au licenciement pour **négligence caractérisée** ayant causé une violation de données. L'employeur doit fournir les **moyens techniques** nécessaires et **former** les salariés aux bonnes pratiques. La **responsabilité partagée** impose une collaboration étroite pour prévenir les cybermenaces.

Définition

Les **obligations de cybersécurité du salarié** en télétravail désignent l'ensemble des règles et bonnes pratiques que le salarié doit respecter pour garantir la **sécurité des systèmes d'information** et la **protection des données** de l'entreprise lorsqu'il travaille hors des locaux. Ces obligations découlent du **pouvoir de direction** de l'employeur, de la charte informatique, du RGPD et de la convention du 20 octobre 2020 qui prévoit que le salarié doit respecter les règles de **confidentialité et de sécurité** définies par l'entreprise. Les contrôles de sécurité informatique encadrent la mise en oeuvre par l'employeur.

Questions fréquentes

Comment sécuriser le réseau Wi-Fi domestique ?

Par un mot de passe robuste et un chiffrement WPA3 ou WPA2. Les réseaux publics non sécurisés doivent être évités. Cette sécurisation du réseau domestique est essentielle pour protéger les communications professionnelles transitant entre le domicile du télétravailleur et les systèmes de l'entreprise.

Faut-il signaler les incidents de sécurité ?

Oui immédiatement. Le salarié doit signaler tout incident de sécurité au service informatique. La rapidité du signalement est déterminante pour limiter l'impact d'une cyberattaque. Cette obligation découle du devoir de loyauté et de la charte informatique signée par le salarié.

Le salarié peut-il connecter des périphériques personnels ?

Non. La séparation stricte de l'usage professionnel et personnel impose d'éviter de connecter des périphériques personnels (clés USB, disques durs) au matériel de l'entreprise. Cette interdiction prévient la propagation de logiciels malveillants et la fuite de données professionnelles.

Que risque le salarié en cas de négligence caractérisée ?

Une faute disciplinaire pouvant aller jusqu'au licenciement pour négligence caractérisée ayant causé une violation de données. L'employeur doit toutefois prouver que le salarié avait été dûment informé et formé aux règles applicables avant de prononcer une sanction.

Quel matériel utiliser en télétravail ?

Exclusivement le matériel fourni par l'employeur. L'utilisation du matériel professionnel pour le travail est obligatoire. L'employeur doit fournir les moyens techniques nécessaires conformément à la convention du 20 octobre 2020 et former les salariés aux bonnes pratiques de cybersécurité.

Quelles sont les obligations de cybersécurité du salarié en télétravail ?

Le salarié doit respecter l'ensemble des règles de sécurité informatique définies par l'employeur, conformément à la convention du 20 octobre 2020 et à la charte informatique. Cela inclut l'utilisation exclusive du matériel professionnel, la connexion VPN sécurisée et le respect de la politique de mots de passe.

Conditions d’exercice

Les obligations de cybersécurité du salarié en télétravail couvrent plusieurs domaines complémentaires.

Obligation	Détail
Matériel professionnel	Utiliser exclusivement le matériel fourni par l'employeur pour le travail
Connexion sécurisée	Se connecter via le VPN de l'entreprise pour tout accès aux ressources internes
Authentification	Utiliser l'authentification multifacteur lorsqu'elle est mise en place
Mots de passe	Respecter la politique de mots de passe (complexité, renouvellement, non-partage)
Verrouillage	Verrouiller systématiquement la session en cas d'absence, même brève
Signalement	Signaler immédiatement tout incident de sécurité au service informatique
Confidentialité	Ne pas laisser de documents professionnels accessibles à des tiers au domicile

Modalités pratiques

L'employeur doit fournir les moyens et encadrer les pratiques de cybersécurité en télétravail.

Mesure employeur	Détail
Charte informatique	Document écrit détaillant les obligations et sanctions, signé par le salarié
Formation initiale	Session de sensibilisation à la cybersécurité avant le début du télétravail
Formation continue	Rappels réguliers sur les menaces actuelles (phishing, ransomware)
Support technique	Assistance informatique accessible à distance pendant les horaires de travail
Mises à jour	Déploiement automatique des correctifs de sécurité sur le matériel professionnel
Tests de phishing	Campagnes de simulation pour évaluer la vigilance des salariés
Procédure d'incident	Protocole clair de signalement et de réponse en cas d'incident

Pratiques et recommandations

Séparer strictement l'usage professionnel et personnel du matériel informatique, en évitant de connecter des périphériques personnels (clés USB, disques durs) au matériel de l'entreprise. **Sécuriser** le réseau Wi-Fi domestique avec un mot de passe robuste et un chiffrement WPA3 ou WPA2, et éviter les réseaux publics non sécurisés.

Ne jamais stocker de données professionnelles sur des supports personnels ou des services cloud non approuvés par l'entreprise. **Vérifier** systématiquement l'identité de l'expéditeur avant d'ouvrir une pièce jointe ou de cliquer sur un lien, en particulier pour les demandes urgentes ou inhabituelles.

Signaler immédiatement tout comportement suspect (email frauduleux, tentative d'accès non autorisé, dysfonctionnement du matériel) au service informatique, même en cas de doute, conformément au cadre général du télétravail. La rapidité du signalement est déterminante pour limiter l'impact d'une cyberattaque. **Participer** activement aux formations de sensibilisation et appliquer les recommandations du service informatique.

Cadre juridique

Référence	Objet
Convention interprofessionnelle du 20 octobre 2020	Obligations de confidentialité et sécurité en télétravail
Règlement (UE) 2016/679 (RGPD)	Protection des données personnelles, obligations de sécurité
Art. L.261-1 du Code du travail	Traitement de données et surveillance des salariés
Art. L.312-1 du Code du travail	Obligation de sécurité de l'employeur
Loi du 1er août 2018	Mise en oeuvre du RGPD au Luxembourg (CNPD)

La négligence caractérisée en matière de cybersécurité (partage de mot de passe, connexion sur réseau non sécurisé ayant causé une fuite de données) peut justifier un licenciement pour faute grave. L'employeur doit toutefois prouver que le salarié avait été dûment informé et formé aux règles applicables.