Comment gérer les contrôles de sécurité informatique en télétravail ?

Réponse courte

L'employeur a l'obligation d'assurer la **sécurité des systèmes d'information** utilisés en télétravail, conformément à l'art. L.312-1 du Code du travail et à la convention interprofessionnelle du 20 octobre 2020. Les contrôles de sécurité informatique doivent être **proportionnés**, déclarés à la CNPD lorsqu'ils impliquent un traitement de données personnelles, et portés à la connaissance du salarié avant leur mise en oeuvre.

L'art. L.261-1 du Code du travail encadre strictement la **surveillance des salariés** à des fins de contrôle. L'employeur peut surveiller l'utilisation des outils professionnels (journaux de connexion, antivirus, filtrage) mais ne peut pas accéder aux données personnelles du salarié ni surveiller son activité en temps réel de manière disproportionnée. Le **règlement intérieur** ou la charte informatique doit préciser les moyens de contrôle autorisés et les sanctions encourues.

Définition

Les contrôles de sécurité informatique en télétravail désignent l'ensemble des mesures techniques et organisationnelles mises en oeuvre par l'employeur pour protéger les **systèmes d'information** et les **données professionnelles** lorsque le salarié travaille à distance. Ils s'inscrivent dans l'obligation de sécurité de l'employeur tout en respectant le droit à la **vie privée** du salarié. Les obligations RGPD spécifiques au télétravail complètent ce cadre.

Conditions d’exercice

Les contrôles de sécurité informatique en télétravail sont soumis à un cadre juridique précis.

Condition	Détail
Proportionnalité	Les contrôles doivent être proportionnés au risque identifié (art. L.261-1)
Information préalable	Le salarié doit être informé des dispositifs de contrôle avant leur activation
Déclaration CNPD	Tout traitement de données personnelles lié au contrôle doit être déclaré
Finalité légitime	Le contrôle doit viser la sécurité des systèmes, pas la surveillance de la productivité
Séparation	Distinction entre données professionnelles (contrôlables) et données personnelles (protégées)
Base contractuelle	Les règles de contrôle doivent figurer dans la charte informatique ou l'avenant

Modalités pratiques

La mise en place des contrôles de sécurité en télétravail suit un processus structuré.

Mesure	Détail
VPN obligatoire	Imposer l'utilisation d'un réseau privé virtuel pour tout accès aux ressources de l'entreprise
Authentification renforcée	Mettre en place l'authentification multifacteur (MFA) pour les accès à distance
Chiffrement	Chiffrer les données stockées sur le matériel professionnel utilisé à domicile
Journalisation	Activer les logs de connexion et d'accès aux applications sensibles
Antivirus et mises à jour	Garantir la mise à jour automatique des logiciels de sécurité
Politique BYOD	Définir les règles si le salarié utilise son matériel personnel

Pratiques et recommandations

Rédiger une charte de sécurité informatique spécifique au télétravail précisant les obligations du salarié et les moyens de contrôle autorisés.

Former les salariés aux bonnes pratiques de cybersécurité à domicile (mots de passe, phishing, Wi-Fi sécurisé) avant le début du télétravail.

Séparer clairement les outils professionnels des outils personnels pour faciliter les contrôles tout en préservant la vie privée du salarié.

Réaliser des audits de sécurité périodiques sur les équipements utilisés en télétravail sans accéder aux contenus personnels du salarié, conformément au cadre général du télétravail.

Cadre juridique

Référence	Objet
Art. L.261-1 Code du travail	Encadrement de la surveillance des salariés et protection des données
Art. L.312-1 Code du travail	Obligation de sécurité de l'employeur
Convention interprofessionnelle du 20 octobre 2020, art. 7	Sécurité informatique et protection des données en télétravail
Règlement (UE) 2016/679 (RGPD)	Principes de proportionnalité et de minimisation des données

La CNPD a rappelé que les outils de surveillance en temps réel de l'écran ou de la webcam du salarié en télétravail sont en principe disproportionnés et contraires au RGPD. L'employeur qui met en place de tels dispositifs sans justification impérieuse s'expose à des sanctions administratives et pénales.