Politique de Télétravail Sécurisé

1. Objectif

E1: Définir les règles et bonnes pratiques pour assurer la sécurité des systèmes d'information et des données lors du télétravail.

2. Champ d'application

E2: Cette politique s'applique à tous les employés, prestataires et partenaires ayant un accès distant aux systèmes d'information de l'entreprise.

3. Exigences de Sécurité pour le Télétravail

E3: Utilisation obligatoire d'un VPN pour accéder aux ressources de l'entreprise.
E4: Authentification multi-facteurs (MFA) requise pour toutes les connexions distantes.
E5: Interdiction d'utiliser des appareils personnels non sécurisés pour les activités professionnelles.
E6: Mise à jour régulière des systèmes d'exploitation et des logiciels de sécurité.
E7: Chiffrement des données stockées et transmises via des connexions sécurisées.

4. Bonnes Pratiques de Sécurité

E8: Sensibilisation des employés aux risques liés au phishing et aux cyberattaques.
E9: Obligation de verrouiller les sessions en cas d'absence prolongée.
E10: Utilisation exclusive des outils collaboratifs approuvés par l'entreprise.
E11: Signalement immédiat de tout incident ou comportement suspect au support IT.

5. Gestion des Accès et Conformité

E12: Droits d'accès limités en fonction des besoins métier.
E13: Audit régulier des accès distants et des connexions VPN.
E14: Respect des réglementations en vigueur (RGPD, ISO 27001, NIS2, etc.).

6. Surveillance et Amélioration Continue

E15: Tests réguliers des dispositifs de sécurité du télétravail.
E16: Mise à jour continue des directives en fonction des nouvelles menaces.
E17: Évaluation périodique de la politique pour assurer son efficacité.

Cette politique est révisée au moins une fois par an ou après toute évolution majeure des risques.