					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P09S					Titre du document : **Politique de télétravail**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Articles 6.1, 6.2, 8	
ISO/IEC 27002:2022	Mesure 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Directive UE NIS2	Articles 21(2)(b), 21(2)(h)	NIS2
Règlement UE DORA	Article 9	DORA
COBIT 2019	DSS05, APO13	COBIT 2019
RGPD de l'UE	Article 32	RGPD

1. Objet

1.1 La présente politique définit les exigences de sécurité applicables aux employés et aux prestataires travaillant à distance, y compris depuis leur domicile, des espaces de travail partagés ou en déplacement.

1.2 Elle vise à protéger la confidentialité, l'intégrité et la disponibilité des informations métier consultées en dehors des environnements contrôlés par l'entreprise.

1.3 La présente politique a pour objet d'assurer la conformité aux normes internationales et de réduire les risques tels que l'accès non autorisé, la perte de données et l'interruption de service.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel (employés, prestataires, consultants et travailleurs temporaires) qui accède aux systèmes, réseaux ou données de l'entreprise lorsqu'il travaille hors site.

2.2 Elle couvre :

2.2.1 l'utilisation des équipements fournis par l'entreprise et des équipements personnels

2.2.2 l'accès via un réseau privé virtuel (VPN), un bureau à distance ou des services en nuage

2.2.3 le traitement sécurisé des informations en dehors des locaux de l'entreprise

2.2.4 la surveillance, la gestion des exceptions et l'application de la politique

2.3 Elle s'applique au télétravail à temps plein comme à temps partiel, y compris à l'accès à distance ponctuel.

3. Objectifs

3.1 Prévenir tout accès non autorisé aux systèmes de l'entreprise ou aux données sensibles pendant le télétravail.

3.2 Veiller à ce que les équipements et les liaisons de communication utilisés en dehors du bureau respectent les exigences minimales de sécurité.

3.3 Maintenir la maîtrise des privilèges d'accès à distance et de la surveillance associée.

3.4 Fournir des orientations claires aux employés et aux responsables pour garantir des pratiques de télétravail sécurisées.

3.5 Respecter les exigences d'ISO, de NIS2, du RGPD, de DORA et de COBIT en matière de télétravail et de mobilité.

4. Rôles et responsabilités

4.1 Directeur général

4.1.1 Approuve les modalités de télétravail et supervise la conformité.

4.1.2 Fait remonter les incidents de sécurité ou les cas répétés de non-conformité.

4.1.3 Examine les dérogations et veille au suivi des incidents.

4.2 Responsable informatique ou prestataire externe de services informatiques

4.2.1 Met en place un accès à distance sécurisé (par exemple, VPN, authentification multifacteur).

4.2.2 Assure la mise en œuvre technique de la sécurité des terminaux, du chiffrement et des configurations des équipements.

4.2.3 Assiste les utilisateurs et examine tout incident technique de sécurité.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1 Revue annuelle de la politique

9.1.1 Le directeur général et le support informatique doivent revoir la présente politique chaque année afin de tenir compte des évolutions technologiques, de l'organisation du travail et du cadre juridique.

9.2 Déclencheurs de mise à jour anticipée

9.2.1 Une revue immédiate est requise après :

9.2.1.1 un incident majeur de sécurité lié au télétravail

9.2.1.2 des modifications des exigences de NIS2, du RGPD ou de DORA

9.2.1.3 une transition vers une nouvelle technologie d'accès à distance (par exemple, une autre plateforme VPN)

9.3 Gestion des versions et archivage

9.3.1 Toutes les versions de la présente politique doivent être :

9.3.1.1 datées et approuvées par le directeur général

9.3.1.2 identifiées par un numéro de version

9.3.1.3 archivées pendant au moins trois ans

9.4 Communication au personnel

9.4.1 Les mises à jour de la politique doivent être communiquées à tous les utilisateurs à distance. Une attestation de prise de connaissance est requise pour toute modification significative.

10. Politiques associées et articulations

10.1 La présente politique s'articule avec les documents suivants, qu'elle complète :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : définit qui autorise et supervise l'accès à distance

10.1.2 P4S – Politique de contrôle d'accès : définit la mise en place d'un accès à distance sécurisé et les procédures de révocation

10.1.3 P6S – Politique de gestion des risques : assure le suivi et l'évaluation des risques liés à l'accès hors site

10.1.4 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : forme les utilisateurs aux risques du télétravail et aux bonnes pratiques

10.1.5 P30S – Politique de réponse aux incidents : encadre la réponse aux incidents d'accès à distance tels que les fuites d'identifiants ou la perte d'équipement

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 6.1 – Planification fondée sur les risques pour les scénarios d'accès à distance

11.1.2 Article 6.2 – Traite des responsabilités des ressources humaines dans les contextes mobiles et à distance

11.1.3 Article 8.1 – Planification opérationnelle et contrôle des processus à distance

11.2 ISO/IEC 27002

11.2.1 Mesure 6.7 – Fournit des orientations pratiques sur la sécurité du travail à distance et mobile

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Contrôle de l'accès à distance, protections de session et surveillance de la sécurité

11.3.2 AC-2 – Gestion des comptes pour les utilisateurs hors site

11.4 RGPD de l'UE

11.4.1 Article 32 – Exige la protection des données « dès la conception et par défaut », y compris dans les environnements à distance

11.5 Directive UE NIS2

11.5.1 Article 21(2)(b) – Exige une utilisation sécurisée des systèmes de réseaux et d'information

11.5.2 Article 21(2)(h) – Prévoit des mesures de sécurité liées aux ressources humaines, y compris des contrôles hors site

11.6 Règlement UE DORA

11.6.1 Article 9 – Exige que les entités financières maintiennent la résilience des TIC dans tous les modes opératoires, y compris l'accès à distance

11.7 COBIT 2019

11.7.1 DSS05 – Gestion des services de sécurité : inclut la protection des terminaux et des pratiques de télétravail sécurisées

11.7.2 APO13 – Sécurité gérée : garantit une attribution sécurisée des accès et une supervision des risques pour les accès mobiles et à distance