					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P09					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**

1. Objet

1.1 La présente politique définit les exigences obligatoires applicables à l'exercice sécurisé du télétravail, y compris l'utilisation des systèmes de l'organisation, l'accès aux données et l'exécution des activités professionnelles en dehors des locaux de l'entreprise.

1.2 Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels accessibles à distance et établit des contrôles destinés à atténuer les risques liés aux environnements de travail distribués.

1.3 La présente politique répond à la mesure 6.7 de l'annexe A de l'ISO/IEC 27001:2022 en mettant en œuvre des mesures de protection techniques et procédurales adaptées aux conditions de travail à distance.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel autorisé à travailler à distance, y compris :

2.1.1 les employés (à temps plein, à temps partiel, contractuels)

2.1.2 les prestataires externes de services informatiques, les consultants et les fournisseurs

2.1.3 le personnel temporaire et les membres des équipes projet disposant d'un accès à distance approuvé

2.2 Elle couvre :

2.2.1 l'accès aux systèmes d'information de l'organisation via un réseau privé virtuel (VPN) ou des outils d'accès à distance approuvés

2.2.2 le traitement des informations sensibles et réglementées en dehors des sites sécurisés

2.2.3 l'utilisation d'équipements appartenant à l'organisation ou d'équipements personnels autorisés (BYOD)

2.2.4 les protections physiques et logiques dans les environnements distants

2.3 La présente politique s'applique dans toutes les zones géographiques et tous les fuseaux horaires où l'organisation autorise le télétravail, qu'il soit régulier, ponctuel ou mis en œuvre dans le cadre d'événements de continuité d'activité.

3. Objectifs

3.1 Garantir que seules les personnes autorisées puissent accéder à distance aux systèmes internes et aux informations.

3.2 Imposer le chiffrement, l'authentification multifacteur et les protections des terminaux sur l'ensemble des moyens d'accès à distance.

3.3 Maintenir un niveau de sécurité adapté face aux menaces telles que le phishing, les logiciels malveillants, l'exfiltration de données et l'exposition non autorisée des systèmes.

3.4 Encadrer les modalités de transmission, de stockage ou d'impression des données sensibles dans des environnements hors site.

3.5 Intégrer des mesures de sécurité physique réduisant la visibilité et l'observation non autorisée pendant les sessions à distance.

3.6 Respecter les exigences réglementaires internationales relatives à l'accès à distance aux données, y compris le RGPD, NIS2 et DORA.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Approuve la présente politique et veille à ce que les ressources nécessaires soient allouées et qu'elle soit intégrée aux opérations RH, informatiques et de sécurité.

4.1.2 Autorise les critères d’éligibilité au télétravail au niveau de l’organisation et leur applicabilité aux unités opérationnelles.

4.2 RSSI / responsable du SMSI

4.2.1 Est responsable de la présente politique, en assure la maintenance et veille à son alignement avec le niveau de risque et les exigences réglementaires.

4.2.2 Définit les contrôles de sécurité applicables à l’accès à distance (par exemple : chiffrement, protection des terminaux, délais d’expiration de session).

4.2.3 Approuve la gestion des dérogations et surveille l’efficacité des contrôles.

[... 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 Fréquence de revue

9.1.1 La présente politique doit être revue annuellement, ou plus fréquemment en cas de :

9.1.1.1 introduction de nouvelles technologies d’accès à distance

9.1.1.2 extension significative du télétravail (par exemple : initiatives de travail hybride)

9.1.1.3 apparition de nouvelles menaces, vulnérabilités ou incidents liés aux environnements distants

9.1.1.4 évolution des cadres juridiques ou réglementaires applicables

9.2 Responsable et processus de revue

9.2.1 Le propriétaire de la politique est le RSSI. La revue doit être coordonnée avec :

9.2.1.1 l’exploitation et l’architecture informatiques

9.2.1.2 les ressources humaines et les services généraux (pour les implications opérationnelles et liées à l’espace de travail)

9.2.1.3 le délégué à la protection des données (pour la vie privée et les contrôles relatifs aux données transfrontalières)

9.2.2 Les mises à jour de la politique doivent :

9.2.2.1 être approuvées par le comité de pilotage de la sécurité de l’information (ISSC)

9.2.2.2 être communiquées à l’ensemble du personnel et des prestataires concernés

9.2.2.3 être intégrées aux supports d’intégration et de formation de rappel

9.3 Contrôle documentaire et diffusion

9.3.1 La politique doit inclure la gestion des versions, la date d’entrée en vigueur et l’historique des modifications.

9.3.2 Les versions remplacées doivent être conservées conformément à la politique de gestion documentaire (P14).

9.3.3 Les versions révisées doivent déclencher une nouvelle prise de connaissance obligatoire pour les utilisateurs éligibles au télétravail.

10. Politiques associées et articulations

10.1 La présente politique s’applique conjointement avec :

10.1.1 P1 – Politique de sécurité de l’information : établit le référentiel de base applicable au traitement sécurisé des actifs dans tous les environnements de travail, y compris à distance.

10.1.2 P3 – Politique d’utilisation acceptable : encadre l’utilisation appropriée des équipements et systèmes de l’organisation pendant les sessions de télétravail.

10.1.3 P4 – Politique de contrôle d’accès : garantit que les privilèges d’accès à distance respectent le principe du moindre privilège et des mécanismes d’authentification appropriés.

10.1.4 P6 – Politique de gestion des risques : définit la manière dont les risques liés au télétravail sont identifiés, traités et surveillés dans le SMSI.

10.1.5 P12 – Politique de gestion des actifs : impose l'inventaire et la gestion de configuration de tous les équipements utilisés à distance.

10.1.6 P22 – Politique de journalisation et de surveillance : garantit que les sessions à distance sont surveillées, auditées et conservées conformément aux exigences de conformité.

10.1.7 P14 – Politique de conservation et d'élimination des données : définit les règles de traitement des données applicables au télétravail, y compris pour les supports amovibles et l'élimination des équipements.

10.2 Ces politiques garantissent collectivement que le télétravail est sécurisé, conforme et applicable dans l'ensemble des fonctions et des zones géographiques.

11. Normes et référentiels de référence

11.1 La présente politique s'aligne sur des référentiels internationalement reconnus en matière de sécurité, de protection des données et de gestion des risques liés aux TIC afin de garantir des pratiques de télétravail sécurisées, traçables et conformes.

11.2 ISO/IEC 27001

11.2.1 Clause 6.1.3 – Planification du traitement des risques : la présente politique contribue au traitement des risques liés à l'accès à distance et aux environnements de travail distribués.

11.2.2 Clause 8.1 – Planification et maîtrise opérationnelles : impose la mise en œuvre de contrôles pour les systèmes accessibles en dehors des locaux de l'organisation.

11.2.3 Annexe A, mesure 6.7 – Télétravail : la présente politique couvre intégralement les contrôles requis en matière de sécurité de l'information lorsque le personnel travaille en dehors des locaux de l'organisation, y compris les protections physiques et logiques, la gouvernance des accès et la surveillance des comportements utilisateurs.

11.3 ISO/IEC 27002:2022 – Mesure 6

11.3.1 Cette mesure impose des mesures de protection procédurales et techniques pour le télétravail. Elle comprend des exigences relatives à la sécurité des équipements, aux méthodes d'accès, au traitement des données, aux protections environnementales et à la gestion des tiers, toutes mises en œuvre par la présente politique.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Accès à distance) : pris en charge directement au moyen des contrôles VPN, de l'authentification multifacteur, de la journalisation des sessions et de l'autorisation d'accès fondée sur les rôles pour les utilisateurs distants.

11.4.2 AC-2 (Gestion des comptes) : encadre l'éligibilité à l'accès, l'attribution des privilèges distants et la désactivation des comptes.

11.4.3 SC-12 à SC-13 (Protection cryptographique, établissement de clés cryptographiques) : mis en œuvre par l'usage obligatoire des VPN et du chiffrement intégral du disque pour les terminaux distants.

11.4.4 MP-5 (Protection du transport des supports) et PE-18 (Emplacement des composants du système d'information) : les règles de télétravail imposent la protection du transport et des mesures de protection physiques dans les environnements hors site.

11.4.5 AU-2, AU-6 : la journalisation et la surveillance des sessions distantes soutiennent les exigences d'audit et de réponse aux incidents.

11.5 RGPD de l'UE (2016/679)

11.5.1 Article 32 – Sécurité du traitement : la présente politique impose les contrôles d'accès à distance, de chiffrement et de journalisation nécessaires à la sécurisation des données à caractère personnel accessibles ou traitées à distance.

11.5.2 Article 5(1)(f) : garantit que les données à caractère personnel consultées hors site sont protégées contre tout traitement non autorisé ou illicite ainsi que contre toute perte accidentelle.

11.5.3 Considérant 39 : met l'accent sur la limitation des accès, l'intégrité et la confidentialité, en particulier lorsque les équipements quittent des locaux sécurisés.

11.6 Directive NIS2 de l'UE (2022/2555)

11.6.1 Article 21(2)(a, b, d) : impose la sécurisation des accès à distance dans le cadre du dispositif de gestion des risques liés aux TIC de l'organisation. La présente politique répond à cette exigence en prévoyant des mesures de sécurité couvrant le contrôle d'accès, la sécurité des données et les politiques organisationnelles applicables aux environnements distants.

11.6.2 Article 21(3) : encourage la sensibilisation à la sécurité et l'application de la politique auprès du personnel travaillant en dehors des locaux centraux.

11.7 DORA de l'UE (2022/2554)

11.7.1 Article 5 – Cadre de gouvernance et de contrôle interne : la présente politique répond aux attentes en matière de maîtrise des risques liés aux TIC dans tous les scénarios opérationnels, y compris les modèles hybrides et distants.

11.7.2 Article 8 – Cadre de gestion des risques liés aux TIC : les risques liés à l'accès à distance sont identifiés, atténués et gouvernés au moyen des contrôles techniques et organisationnels imposés par la présente politique.

11.7.3 Article 9 – Dispositifs de partage d'informations : protège contre les fuites d'informations à distance au sein des réseaux numériques de résilience opérationnelle.

11.8 COBIT 2019

11.8.1 DSS01 – Gestion des opérations : la présente politique soutient la continuité sécurisée des opérations métier, quel que soit le lieu physique.

11.8.2 BAI06 – Gestion des changements informatiques et BAI09 – Gestion des actifs : garantissent que les équipements de télétravail sont suivis, configurés de manière sécurisée et traités comme des actifs critiques.

11.8.3 APO13 – Gestion de la sécurité : promeut un cadre de gouvernance de la sécurité défini pour les environnements distants.

11.8.4 MEA03 – Surveiller, évaluer et apprécier la conformité : établit que l'activité de télétravail doit être journalisée, revue et auditée.