					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P10S					Titre du document : **Politique de bureau propre et d'écran verrouillé**							
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	Clauses 7.2, 8	
ISO/IEC 27002:2022	Mesure 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Directive NIS2 de l'UE	Article 21(2)(d)	
Règlement DORA de l'UE	Article 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
RGPD de l'UE	Article 32	

1. Objet

1.1 La présente politique établit des règles contraignantes visant à maintenir un environnement de travail sécurisé en garantissant que les bureaux, postes de travail et écrans d'affichage ne laissent apparaître aucune information confidentielle lorsqu'ils sont laissés sans surveillance.

1.2 Elle a pour objectif principal de prévenir tout accès non autorisé à des informations sensibles résultant de documents imprimés laissés sans surveillance, d'écrans non verrouillés ou de supports amovibles égarés, tant dans les environnements de bureau physiques que dans les lieux de télétravail.

1.3 Les pratiques de bureau propre et d'écran verrouillé définies dans la présente politique renforcent la capacité de l'organisation à satisfaire aux exigences de certification ISO/IEC 27001 en réduisant les risques d'exposition évitables. Elles démontrent également aux clients, partenaires et auditeurs que l'organisation applique la sécurité de l'information avec rigueur, y compris dans des environnements disposant de ressources limitées.

1.4 La présente politique soutient une culture de responsabilité et de sensibilisation, en veillant à ce que l'ensemble du personnel, indépendamment de son rôle ou de son niveau d'expertise technique, comprenne sa responsabilité dans la protection des informations de l'entreprise et des clients contre l'exposition visuelle, le vol ou la perte.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les salariés, prestataires, stagiaires et personnels temporaires utilisant des postes de travail, bureaux ou appareils mobiles appartenant à l'entreprise ou mis à leur disposition à titre individuel

2.1.2 Tous les lieux physiques utilisés pour les activités de l'entreprise, y compris les bureaux dédiés, les espaces de coworking et les espaces de travail à domicile ou à distance

2.1.3 Tous les équipements numériques dotés de capacités d'affichage, y compris les ordinateurs fixes, ordinateurs portables, tablettes et moniteurs externes utilisés à des fins professionnelles

2.2 La politique s'étend à tout actif physique ou numérique susceptible d'afficher, de contenir ou de transmettre des informations sensibles, notamment :

2.2.1 Les documents imprimés ou notes manuscrites

2.2.2 Les clés USB, CD et disques durs externes

2.2.3 Les téléphones mobiles utilisés pour la messagerie professionnelle ou le courrier électronique

2.2.4 Les écrans d’ordinateur et projecteurs connectés aux systèmes de travail

2.3 La présente politique demeure applicable en dehors des heures normales de travail et lors d’opérations non standard (par exemple, maintenance hors heures ouvrées ou activités de réponse d’urgence).

3. Objectifs

3.1 Mettre en œuvre des contrôles pratiques et cohérents afin qu’aucune information sensible ne reste exposée sur les bureaux, écrans ou dans les espaces communs.

3.2 Réduire le risque d’accès non autorisé, qu’il provienne de sources internes (par exemple, accès non intentionnel par d’autres salariés) ou de menaces externes (par exemple, visiteurs, personnel de nettoyage ou prestataires).

3.3 Renforcer les restrictions d’accès physique et logique en imposant au personnel de sécuriser activement les documents de travail et de verrouiller les ordinateurs lorsqu’ils sont laissés sans surveillance.

3.4 Développer la sensibilisation du personnel à la sécurité au regard des pratiques de travail sécurisées et fournir des règles simples et contraignantes applicables aux opérations quotidiennes, quel que soit le lieu de travail.

3.5 Assurer l’alignement avec l’Annexe A de l’ISO/IEC 27001, mesure 7.7, ainsi qu’avec les lignes directrices de mise en œuvre de l’ISO/IEC 27002 concernant les exigences de bureau propre et d’écran verrouillé.

3.6 Veiller à ce que l’organisation soit en mesure de démontrer sa diligence raisonnable et sa préparation à l’audit sans nécessiter une infrastructure de niveau entreprise.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Est responsable de la présente politique et veille à ce qu’elle soit correctement communiquée, comprise et respectée par l’ensemble des salariés et prestataires.

4.1.2 Est chargé d’approuver toute dérogation à la politique, de traiter les manquements et de superviser la formation relative aux pratiques de travail sécurisées.

4.1.3 Doit réaliser ou déléguer des contrôles ponctuels réguliers (au moins trimestriels) afin de confirmer que les espaces de travail physiques et numériques répondent aux exigences de la politique.

4.2 Salarié désigné (le cas échéant)

4.2.1 Peut se voir confier la responsabilité de mettre en œuvre des configurations techniques (par exemple, paramètres de temporisation de verrouillage de l’écran) ou de distribuer des dispositifs de stockage physique (par exemple, tiroirs verrouillables).

4.2.2 Appuie le DG en signalant toute non-conformité, en diffusant des rappels relatifs à la sécurité des espaces de travail et en assurant le suivi des actions correctives lorsqu’un écart est identifié.

4.2.3 Contribue à garantir que tous les salariés disposent, lorsque cela est réalisable, de mécanismes de verrouillage appropriés ou d’espaces de stockage sécurisés.

[... 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 Le DG doit procéder à une revue de la présente politique au moins une fois par an et à la suite de l’un des événements suivants :

9.1.1 Mise en service de nouveaux espaces de bureau, appareils ou systèmes partagés

9.1.2 Évolutions des exigences légales ou de certification applicables

9.1.3 Constats issus d'audits, d'évaluations des risques ou d'incidents de sécurité de l'information

9.2 Les mises à jour intermédiaires doivent être communiquées à l'ensemble des salariés par courrier électronique, avec accusé de réception obligatoire.

9.3 Les versions antérieures de la présente politique doivent être conservées en sécurité et rester auditables afin de démontrer l'alignement continu avec l'ISO/IEC 27001 et les référentiels associés.

10. Politiques associées et articulations

10.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : précise l'autorité du DG pour appliquer et auditer les comportements liés aux espaces de travail physiques et numériques.

10.2 P4S – Politique de contrôle d'accès : soutient la mise en œuvre technique des pratiques de verrouillage d'écran et de connexion sécurisée aux postes de travail.

10.3 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : renforce la formation comportementale nécessaire au respect de la politique.

10.4 P17S – Politique de protection des données et de la vie privée : définit les obligations relatives au traitement et à la protection des données à caractère personnel et des données sensibles en conformité avec le RGPD.

10.5 P30S – Politique de réponse aux incidents : fournit le cadre d'escalade et de réponse lorsqu'un manquement entraîne une exposition de données ou une violation de données.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 7.2 : exige que l'ensemble du personnel soit sensibilisé à ses responsabilités en matière de sécurité, y compris aux mesures de protection physiques.

11.1.2 Clause 8.1 : les contrôles opérationnels doivent garantir des protections physiques et logiques appropriées.

11.2 ISO/IEC 27002

11.2.1 Mesure 7.7 : fournit des orientations détaillées sur la définition, la communication et l'application des exigences de bureau propre et d'écran verrouillé.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2 : établit les attentes en matière de contrôle d'accès physique, y compris le comportement du personnel dans les environnements sécurisés.

11.3.2 AC-11 : impose une fonction de verrouillage de session pour les postes de travail afin d'empêcher toute visualisation ou interaction non autorisée.

11.4 RGPD de l'UE

11.4.1 Article 32 : exige que les organisations protègent les données à caractère personnel au moyen de mesures de protection physiques et techniques, y compris pour les postes de travail et les documents.

11.5 Directive NIS2 de l'UE

11.5.1 Article 21(2)(d) : exige que les organisations mettent en œuvre des politiques d'accès physique et logique fondées sur les risques.

11.6 Règlement DORA de l'UE

11.6.1 Article 9(2)(f) : impose des politiques de sécurité des TIC, y compris des pratiques sécurisées d'hygiène de l'espace de travail, pour les opérateurs du secteur financier et leurs chaînes d'approvisionnement.

11.7 COBIT 2019

11.7.1 DSS01.06 : exige des pratiques de protection des actifs, y compris des contrôles physiques sur les espaces de travail et les supports.

11.7.2 DSS05.02 : soutient l’application des pratiques de sécurité des utilisateurs finaux dans l’ensemble des environnements d’exploitation.