					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P10					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	Clause 6.1.3, Clause 8	plan de traitement des risques, planification et maîtrise opérationnelles, et contrôle des espaces de travail sécurisés
ISO/IEC 27002:2022	Mesure 7	contrôles comportementaux et environnementaux visant à sécuriser les informations physiques laissées sans surveillance
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	accès physique, sécurité des prestataires, élimination des supports, verrouillage de session, paramètres de configuration et contrôle des authentificateurs
RGPD de l'UE	Articles 5(1)(f), 32 ; considérant 39	intégrité des données, confidentialité et mesures de protection physiques des données
NIS2 de l'UE	Articles 21(2)(d), 21(3)	politiques relatives à la sécurité physique, au comportement des utilisateurs et à la prévention des fuites
DORA de l'UE	Articles 5, 8, 9	gouvernance interne, TIC et gestion des incidents impliquant la sécurité physique
COBIT 2019	DSS01, DSS05, MEA	gestion des opérations, services de sécurité et surveillance de la conformité

1. Objet

1.1 La présente politique établit des contrôles obligatoires visant à protéger les informations sensibles en imposant un traitement sécurisé de l'information figurant sur les documents physiques, les postes de travail, les écrans et les supports amovibles, tant dans les bureaux que dans les espaces de travail partagés.

1.2 Elle soutient la mesure 7.7 de l'Annexe A de l'ISO/IEC 27001 en imposant des pratiques comportementales et techniques qui atténuent le risque de divulgation non autorisée, de vol ou de perte de données résultant d'informations visibles ou laissées sans surveillance.

1.3 La présente politique renforce la sécurité physique et la sécurité de l'information dans les opérations quotidiennes et contribue à la conformité aux obligations légales, contractuelles et réglementaires applicables.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel intervenant dans des espaces de travail physiques ou y accédant, notamment :

2.1.1 les employés permanents et temporaires ;

2.1.2 les sous-traitants, consultants, fournisseurs et stagiaires ;

2.1.3 les prestataires de services tiers et les visiteurs sur site ayant accès à des informations sensibles.

2.2 Les exigences s'appliquent dans :

2.2.1 les bureaux individuels, box et espaces de travail en open space ;

2.2.2 les salles de réunion et espaces collaboratifs partagés ;

2.2.3 les zones d'impression, comptoirs d'accueil et salles de reprographie ;

2.2.4 les zones où sont utilisés des postes de travail distants ou des bornes partagées.

2.3 La présente politique s'applique également aux environnements de travail temporaires ou hybrides (par exemple, le partage de bureaux) ainsi qu'aux environnements ouverts au public dans lesquels il existe un risque d'observation indiscrète ou de données laissées sans surveillance.

3. Objectifs

3.1 Prévenir tout accès non autorisé à des informations confidentielles, sensibles ou réglementées laissées exposées sous forme physique ou numérique.

3.2 Promouvoir un niveau de sécurité homogène dans tous les environnements de travail grâce à des mesures de protection physiques, à la configuration des postes de travail et au comportement des utilisateurs finaux.

3.3 Réduire le risque d'atteinte à la vie privée, de perte de propriété intellectuelle et d'exfiltration de données causées par la négligence ou l'inattention.

3.4 Intégrer les comportements de bureau propre et d'écran verrouillé dans la culture de l'organisation afin de renforcer la discipline opérationnelle, l'auditabilité et la capacité de justification en cas de contentieux.

3.5 Soutenir la conformité à l'ISO/IEC 27001, à l'article 32 du RGPD, à l'article 15 de NIS2 et aux autres exigences de sécurité physique applicables aux données critiques ou aux données à caractère personnel.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Approuve la présente politique et promeut une culture de sensibilisation à la sécurité dans l'ensemble des unités opérationnelles.

4.1.2 Alloue les ressources appropriées à l'application de la politique, aux campagnes de sensibilisation et aux mécanismes de contrôle physique.

4.2 RSSI / responsable du SMSI

4.2.1 Est responsable de la présente politique et veille à son alignement sur l'ISO/IEC 27001:2022, les exigences d'audit et les stratégies de traitement des risques.

4.2.2 Met en place des programmes de sensibilisation et des contrôles pour garantir une mise en œuvre cohérente sur l'ensemble des sites et dans les contextes de travail hybrides.

4.2.3 Se coordonne avec les services généraux et la DSI afin de garantir la mise en place de mesures de protection physiques appropriées.

[... 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 Calendrier de revue de la politique

9.1.1 La présente politique doit faire l'objet d'une revue :

9.1.1.1 au moins une fois par an ;

9.1.1.2 après toute non-conformité d'audit liée à l'exposition d'un espace de travail ou d'un écran ;

9.1.1.3 à la suite de tout incident physique ou environnemental (par exemple, vol d'équipement, intrusion par suivi de personne autorisée, surveillance) ;

9.1.1.4 lors de la mise en œuvre de nouveaux aménagements de bureaux, politiques relatives aux installations ou modèles d'organisation des espaces de travail (par exemple, partage de bureaux, hubs distants).

9.2 Responsables désignés

9.2.1 Le responsable de la politique est le RSSI ou le responsable du SMSI désigné.

9.2.2 Le processus de revue doit associer :

9.2.2.1 les équipes des installations et de sécurité de l'entreprise ;

9.2.2.2 la DSI et l'infrastructure pour la mise en application liée aux équipements ;

9.2.2.3 les ressources humaines et les affaires juridiques pour l'application comportementale et l'alignement disciplinaire.

9.2.3 Toute mise à jour de la politique doit faire l'objet d'une gestion des versions, être approuvée par le comité de pilotage du SMSI et être diffusée avec une nouvelle prise de connaissance lorsque cela est requis.

9.3 Communication des modifications

9.3.1 Les utilisateurs doivent être informés des mises à jour substantielles via :

9.3.1.1 le centre de politiques de l'intranet ou le portail dédié ;

9.3.1.2 des communications ciblées par courrier électronique ;

9.3.1.3 des rappels lors de l'intégration et des points d'information trimestriels ;

9.3.1.4 des demandes obligatoires d'accusé de réception pour toute nouvelle clause critique d'application.

10. Politiques associées et articulations

10.1 La présente politique est alignée sur les politiques suivantes et les soutient :

10.1.1 P1 – Politique de sécurité de l'information : établit les attentes relatives au comportement des utilisateurs et à la sécurité physique qui fondent la présente politique.

10.1.2 P3 – Politique d'utilisation acceptable : traite de la responsabilité des utilisateurs dans la protection des données et des systèmes, y compris dans les environnements physiques.

10.1.3 P6 – Politique de gestion des risques : intègre les risques liés aux espaces de travail physiques dans l'analyse globale des risques liés à l'information de l'entreprise.

10.1.4 P12 – Politique de gestion des actifs : soutient le suivi et le traitement sécurisé de l'information pour les équipements et supports laissés sur les bureaux.

10.1.5 P13 – Politique de classification et d'étiquetage des données : établit un lien avec l'application du bureau propre pour les documents physiques étiquetés Confidentiel ou Interne.

10.1.6 P14 – Politique de conservation et d'élimination des données : encadre les pratiques de conservation des documents physiques, de destruction et de gestion des bacs.

10.1.7 P22 – Politique de journalisation et de surveillance : peut être utilisée pour surveiller l'état de verrouillage des postes de travail, la durée d'inactivité ou les flux de caméras des espaces de travail lorsque cela est autorisé.

10.2 Ces politiques associées établissent une culture de sécurité intégrée, articulant sensibilisation des utilisateurs, mesures de protection physiques et responsabilité afin de garantir des espaces de travail résilients.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des normes reconnues à l'échelle internationale et sur des exigences légales imposant la protection des informations sensibles dans les environnements physiques et par le comportement des utilisateurs.

11.2 ISO/IEC 27001

11.2.1 Clause 6.1.3 – plan de traitement des risques : soutient la mise en œuvre de contrôles destinés à atténuer les risques physiques et environnementaux, y compris ceux liés au comportement des utilisateurs dans les espaces de travail ouverts.

11.2.2 Clause 8.1 – planification et maîtrise opérationnelles : établit des mesures de protection opérationnelles pour gérer la sécurité des espaces de travail et l'utilisation des équipements.

11.3 ISO/IEC 27002:2022 – Mesure 7

11.3.1 Cette mesure impose des protections comportementales et environnementales afin de prévenir l'accès non autorisé à l'information via des supports, écrans ou documents imprimés laissés sans surveillance. La politique impose la discipline des espaces de travail, l'usage du verrouillage d'écran et l'élimination des documents sensibles.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (autorisations d'accès physique) : pris en compte au travers des restrictions d'accès aux espaces de travail et de l'exigence de stockage verrouillé dans les environnements à haut risque.

11.4.2 PS-7 (sécurité du personnel externe) : appliqué au travers des exigences de bureau propre et d'écran verrouillé étendues aux prestataires et utilisateurs tiers.

11.4.3 MP-6 (assainissement des supports) et AC-11 (verrouillage de session) : mis en œuvre par des procédures d'élimination sécurisée et des temporisations obligatoires de verrouillage d'écran.

11.4.4 CM-6 (paramètres de configuration) et IA-5 (gestion des authentificateurs) : soutiennent la mise en application technique du verrouillage d'écran et du contrôle des sessions sur les terminaux.

11.5 RGPD de l'UE (2016/679)

11.5.1 Article 5(1)(f) : impose l'intégrité et la confidentialité des données à caractère personnel, y compris des protections contre l'exposition physique ou la consultation par des personnes non autorisées.

11.5.2 Article 32 – sécurité du traitement : exige des mesures physiques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte ou la divulgation non autorisée, au moyen notamment des contrôles relatifs aux bureaux et aux écrans.

11.5.3 Considérant 39 : impose de limiter l'accès aux données à caractère personnel aux seules personnes autorisées, ce qui inclut leur sécurisation sous forme physique lorsqu'elles sont laissées sans surveillance.

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

11.6.1 Article 21(2)(d) : exige des politiques et procédures relatives à la sécurité physique et environnementale, y compris des mesures de protection de la sécurité de l'information au niveau du lieu de travail.

11.6.2 Article 21(3) : encourage une culture de sécurité intégrant de bonnes pratiques utilisateurs, la sensibilisation et la prévention des fuites de données involontaires, soutenues par les contrôles comportementaux de la présente politique.

11.7 DORA de l'UE (2022/2554)

11.7.1 Article 5 – gouvernance et contrôle internes : exige que l'ensemble des risques liés aux TIC, y compris les menaces humaines et environnementales, soit encadré par des politiques opposables.

11.7.2 Article 8 – gestion des risques liés aux TIC : impose des mesures de protection dans les contextes numériques et physiques, afin que les utilisateurs à distance, en agence ou sur site ne créent pas d'exposition non maîtrisée.

11.7.3 Article 9 – gestion des incidents : exige que les écarts environnementaux ou comportementaux entraînant une exposition de données soient consignés, classés et traités au moyen d'actions correctives appropriées.

11.8 COBIT 2019

11.8.1 DSS01 – gestion des opérations : garantit une discipline opérationnelle dans la protection des espaces de travail physiques et des systèmes au moyen de contrôles répétables.

11.8.2 DSS05 – gestion des services de sécurité : soutient la protection des données, des équipements et des points d'accès au moyen d'une application fondée sur le comportement, telle que les pratiques de bureau propre.

11.8.3 MEA03 – surveiller, évaluer et apprécier la conformité : encourage l'audit des mesures de protection physiques et de l'adoption de la politique dans les pratiques métier quotidiennes.