					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P01S					Titre du document : **Politique de sécurité de l'information P01S**							
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 5.1, 5.2, 5.3, 6.1, 6.2, 8	Précise l'engagement de la direction, les exigences relatives à la politique, l'attribution des rôles, l'évaluation des risques et la maîtrise opérationnelle
ISO/IEC 27002:2022	Mesures 5.1–5	Précise l'établissement de politiques documentées de sécurité de l'information, l'attribution des rôles, la séparation des tâches et les responsabilités de la direction
NIST SP 800-53 Rév. 5	PM-1, PL-1, CA-1, AC-1	Exigences relatives au plan du programme de sécurité, à la politique de planification de la sécurité, à l'évaluation et à l'autorisation, ainsi qu'au contrôle d'accès
RGPD de l'UE (2016/679)	Article 5(2), Article 32	Principe de responsabilité et mesures de sécurité du traitement, en particulier pour les rôles documentés
Directive NIS2 de l'UE (2022/2555)	Article 21(2)(a)	Exige des mesures de gestion des risques ainsi que la définition des rôles et responsabilités en matière de cyberrisques
DORA de l'UE (2022/2554)	Article 9, Article 10	Exige l'attribution de rôles pour la gestion des risques liés aux TIC et la continuité d'activité
COBIT 2019	EDM03, APO13, DSS05	Assure l'optimisation des risques, la gestion de la sécurité et la gestion des services de sécurité au moyen d'une attribution claire des rôles

1. Objet

1.1 La présente politique formalise l'engagement de l'organisation à protéger les informations des clients et de l'entreprise en définissant clairement les responsabilités et les mesures de sécurité pratiques, adaptées aux organisations ne disposant pas d'équipes informatiques dédiées.

1.2 Elle impose à l'ensemble des employés, prestataires et fournisseurs de services le respect de règles contraignantes, afin de permettre une conformité complète aux exigences de certification ISO/IEC 27001.

1.3 La présente politique permet à l'organisation de renforcer la confiance des clients en démontrant clairement comment leurs informations sont protégées au moyen de responsabilités définies, de processus structurés et d'une responsabilisation forte.

2. Champ d'application

2.1 La présente politique s'applique à toute personne accédant aux données et aux systèmes de l'organisation, ou les administrant, y compris :

2.1.1 Les dirigeants et la direction générale

2.1.2 Les employés, prestataires et stagiaires

2.1.3 Les prestataires externes de services informatiques ou les consultants

2.2 Elle couvre tous les types d'informations, de systèmes et de services, notamment :

2.2.1 Les documents métiers, les données clients, les mots de passe et les courriels

2.2.2 Les équipements informatiques tels que les ordinateurs portables et les téléphones

2.2.3 Les services cloud utilisés pour le stockage de fichiers, la communication ou la gestion financière

2.2.4 Les documents papier conservés dans les locaux de l'entreprise

2.3 La politique s'applique à tous les environnements de travail — sur site, à distance et dans le cloud — et couvre l'ensemble des équipements et logiciels utilisés pour traiter ou stocker les informations de l'entreprise.

3. Objectifs

3.1 Attribuer clairement les responsabilités : garantir qu'une personne est toujours responsable de la sécurité de l'information. En règle générale, il s'agit du directeur général ou de la personne qu'il désigne formellement.

3.2 Protéger les informations des clients et de l'entreprise : mettre en place des mesures de protection fiables et cohérentes afin de prévenir toute utilisation abusive, perte ou vol de données sensibles, y compris les dossiers clients et les informations financières.

3.3 Soutenir la certification ISO/IEC 27001 : permettre à l'organisation de démontrer une conformité complète aux exigences de l'ISO/IEC 27001, afin d'être en mesure de répondre à un audit et d'être éligible à la certification sans nécessiter d'infrastructure complexe.

3.4 Intégrer la sécurité dans les activités de l'entreprise : intégrer la sécurité de l'information dans les tâches et les décisions quotidiennes de l'ensemble de l'organisation.

3.5 Développer la sensibilisation et la culture de sécurité : faire en sorte que chaque employé comprenne et applique les pratiques de sécurité, telles que l'utilisation de mots de passe robustes et le signalement des activités suspectes.

4. Rôles et responsabilités

4.1 Directeur général ou propriétaire de l'entreprise

4.1.1 Assume l'entière responsabilité de la sécurité de l'information.

4.1.2 Approuve et tient à jour la présente politique.

4.1.3 Veille à ce que toutes les tâches de sécurité essentielles soient réalisées directement ou déléguées par écrit.

4.1.4 Vérifie que toute tâche de sécurité déléguée (telle que la gestion des accès ou la réponse aux incidents) est exécutée efficacement.

4.1.5 Est le point de contact par défaut pour toutes les questions de sécurité internes et externes, y compris les audits et les demandes des clients.

4.1.6 Assure, dans le cadre de la revue annuelle, le suivi des progrès réalisés au regard de ces objectifs. Les objectifs doivent être mesurables dans la mesure du possible (par exemple, pourcentage du personnel formé, nombre d'incidents signalés, etc.) et révisés en fonction des constats de sécurité et de l'évolution des risques.

4.2 Employé désigné (le cas échéant)

4.2.1 Peut assister le directeur général dans la gestion des tâches quotidiennes, telles que la création de comptes utilisateurs, la suppression des accès des personnes quittant l'organisation ou la coordination avec le prestataire informatique.

4.2.2 Doit faire l'objet d'une désignation formelle et disposer de l'autorité ainsi que des moyens nécessaires à l'exécution de ses tâches.

4.2.3 Rend compte de toute difficulté au directeur général.

[... 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

9.1.1 La présente politique doit faire l'objet d'une revue par le directeur général (DG) au moins une fois par an afin d'assurer le maintien de la conformité aux exigences de certification ISO/IEC 27001, aux évolutions réglementaires (telles que le RGPD, NIS2 et DORA) et aux besoins évolutifs de l'entreprise.

9.2 Revues intermédiaires

9.2.1 Des revues complémentaires doivent être réalisées en cas de changements significatifs, notamment :

9.2.1.1 Incidents ou violations de sécurité majeurs.

9.2.1.2 Introduction de nouveaux processus métier ou de nouvelles technologies (par exemple, nouveaux logiciels, plateformes de travail à distance ou services cloud).

9.2.1.3 Évolutions des exigences légales ou réglementaires affectant le traitement de l'information.

9.3 Documentation des changements

9.3.1 Toutes les revues de la politique et toutes les modifications doivent être formellement documentées, en précisant clairement la date, la nature des révisions et l'approbation du DG.

9.3.2 Un historique des versions de la politique doit être conservé de manière sécurisée afin de démontrer l'évolution de la politique et la conformité lors des audits.

9.4 Communication des mises à jour

9.4.1 Toute modification de la présente politique doit être communiquée sans délai à l'ensemble des employés, prestataires et tiers concernés.

9.4.2 Les versions mises à jour de la politique doivent être facilement accessibles à l'ensemble des personnes concernées (par exemple, sous forme électronique partagée ou affichées physiquement sur le lieu de travail).

10. Politiques associées et articulations

10.1 La présente politique est étroitement articulée avec d'autres politiques du corpus PME de l'organisation, notamment :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : précise l'attribution des missions et responsabilités en matière de sécurité.

10.1.2 P4S – Politique de contrôle d'accès : définit les règles de gestion sécurisée des accès aux informations de l'entreprise.

10.1.3 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : fournit les orientations essentielles pour la formation et la sensibilisation du personnel.

10.1.4 P17S – Politique de protection des données et de la vie privée : assure la conformité au RGPD et aux autres lois relatives à la protection des données.

10.1.5 P30S – Politique de réponse aux incidents : décrit en détail les actions requises en cas d'incident de sécurité.

10.2 Ces politiques associées fournissent des orientations opérationnelles claires et doivent être mises en œuvre de manière coordonnée afin d'atteindre une conformité complète aux exigences de certification ISO/IEC 27001.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 5.1 – Leadership and Commitment : exige l'engagement de la direction et sa responsabilité quant à l'efficacité de la sécurité de l'information au sein de l'organisation.

11.1.2 Article 5.2 – Information Security Policy : impose des politiques claires et documentées, alignées sur la stratégie de l'organisation et les exigences de conformité.

11.1.3 Article 5.3 – Organizational Roles and Responsibilities : définit une attribution claire des responsabilités en matière de sécurité de l'information au sein de l'organisation, essentielle pour une gouvernance efficace et la conformité en audit.

11.1.4 Article 6.1 – Actions to Address Risks and Opportunities : garantit que les risques pesant sur la sécurité de l'information sont identifiés, évalués et traités de manière systématique.

11.1.5 Article 8.1 – Operational Planning and Control : exige que l'organisation planifie et mette en œuvre les processus nécessaires pour atteindre les objectifs de sécurité de l'information et gérer efficacement les risques associés.

11.2 Mesures ISO/IEC 27002:2022 5.1–5

11.2.1 Annexe A Mesure 5.1 – Policies for Information Security : précise l'établissement et la communication de politiques documentées de sécurité de l'information.

11.2.2 Annexe A Mesure 5.2 – Information Security Roles : clarifie et attribue formellement les rôles et responsabilités en matière de sécurité de l'information aux parties concernées.

11.2.3 Annexe A Mesure 5.3 – Segregation of Duties : impose une séparation claire des tâches afin de réduire les conflits d'intérêts et les risques de fraude dans la gestion des informations sensibles.

11.2.4 Annexe A Mesure 5.4 – Management Responsibilities : impose à la direction de démontrer son engagement en matière de sécurité de l'information par une supervision active et l'allocation de ressources.

11.2.5 Renforce la nécessité de politiques, rôles, responsabilités et structures de gouvernance en matière de sécurité de l'information clairement documentés, afin d'assurer une gestion cohérente et la traçabilité pour l'audit dans l'ensemble de l'organisation.

11.3 NIST SP 800-53 Rév. 5

11.3.1 PM-1 – Information Security Program Plan : exige des stratégies et politiques documentées de gouvernance de la sécurité de l'information, fournissant un cadre pour une mise en œuvre et une gestion cohérentes.

11.3.2 PL-1 – Security Planning Policy : impose une politique de planification de la sécurité à l'échelle de l'organisation afin d'orienter l'exploitation sécurisée et l'alignement stratégique des activités de sécurité de l'information.

11.3.3 CA-1 – Security Assessment and Authorization Policy : exige des rôles clairement définis en matière d'évaluation et d'autorisation afin d'assurer l'efficacité continue et la conformité aux exigences de sécurité de l'information.

11.3.4 AC-1 – Access Control Policy : exige que les organisations définissent clairement, documentent et appliquent les pratiques et responsabilités de gestion des accès.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 5(2) – Principe de responsabilité : exige des organisations qu'elles démontrent leur conformité aux principes de protection des données, y compris au moyen de rôles et de politiques documentés relatifs aux responsabilités en matière de protection des données.

11.4.2 Article 32 – Sécurité du traitement : impose la mise en œuvre de mesures techniques et organisationnelles appropriées, y compris des responsabilités de sécurité clairement définies, afin de protéger les données à caractère personnel contre les violations et les accès non autorisés.

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

11.5.1 Article 21(2)(a) – Mesures de gestion des risques : exige des dispositions de gouvernance claires, y compris des rôles et responsabilités définis en matière de sécurité de l'information, essentielles à une gestion efficace des cyberrisques.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 9 – Gestion des risques liés aux TIC : exige des organisations qu'elles attribuent clairement les rôles et responsabilités relatifs à la gestion des risques liés aux TIC, afin de renforcer la résilience et la préparation à la continuité d'activité.

11.6.2 Article 10 – Continuité d'activité des TIC : exige une responsabilité claire et des rôles structurés pour le maintien de la résilience et de la continuité des TIC, afin de permettre aux organisations de répondre de manière fiable aux perturbations.

11.7 COBIT 2019

11.7.1 EDM03 – Ensure Risk Optimization : souligne l'importance d'une responsabilisation et de rôles clairement définis dans la gestion des risques de l'organisation, en apportant une gouvernance forte et une supervision efficace des risques liés à la sécurité de l'information.

11.7.2 APO13 – Manage Security : exige des organisations qu'elles établissent et communiquent clairement les responsabilités de gestion de la sécurité, afin d'assurer l'alignement avec les objectifs métier et les exigences réglementaires.

11.7.3 DSS05 – Manage Security Services : appelle à des rôles structurés et à des responsabilités claires dans la gestion des services de sécurité, permettant une mise en œuvre cohérente et la vérification de la conformité.