					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P02S					Titre du document : **Politique P02S relative aux rôles et responsabilités en matière de gouvernance**							
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 5	
ISO/IEC 27002:2022	Mesures 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
RGPD de l'UE	Articles 5(2), 32	

1. Objet

1.1 La présente politique définit les modalités d'attribution, de délégation et de gestion des responsabilités de gouvernance de la sécurité de l'information au sein de l'organisation, afin d'assurer une conformité complète à l'ISO/IEC 27001:2022 et aux autres obligations réglementaires.

1.2 Elle établit les responsabilités à chaque niveau et soutient l'efficacité opérationnelle en identifiant clairement le responsable de chaque fonction liée à la sécurité.

1.3 La présente politique renforce la préparation aux audits et la confiance des clients en démontrant l'existence d'une gouvernance formelle de la sécurité, y compris dans les organisations disposant de ressources techniques limitées ou d'une informatique externalisée.

2. Champ d'application

2.1 La présente politique s'applique à toute personne utilisant des systèmes ou traitant des données de l'organisation, y compris :

2.1.1 Les responsables d'activité et les directeurs généraux

2.1.2 Les employés et les prestataires

2.1.3 Les prestataires de services informatiques externes et les consultants

2.2 Elle couvre l'ensemble des systèmes, environnements et services utilisés pour traiter, transmettre ou stocker des informations de l'entreprise ou des clients, y compris :

2.2.1 L'infrastructure informatique de bureau et les équipements de télétravail

2.2.2 Les plateformes cloud et les services de messagerie

2.2.3 Les dossiers physiques et les lecteurs partagés

2.3 Le champ d'application inclut les activités internes et externalisées liées à la gouvernance de la sécurité de l'information.

3. Objectifs

3.1 Établir une responsabilité claire pour l'ensemble des tâches liées à la sécurité, y compris la gestion des politiques, le contrôle d'accès, le traitement des incidents et la supervision.

3.2 Permettre une séparation effective des tâches afin de réduire les conflits d'intérêts et les risques de fraude.

3.3 Garantir que les tâches et rôles liés à la sécurité sont clairement documentés et font l'objet d'une revue régulière.

3.4 Permettre une prise de décision éclairée, une escalade appropriée et une supervision des risques informatiques et de sécurité.

3.5 Soutenir la certification ISO/IEC 27001:2022 et renforcer la confiance des clients, partenaires et auditeurs.

4. Rôles et responsabilités

4.1 Directeur général / Responsable d'activité

4.1.1 Assume l'entière responsabilité de la mise en œuvre et de la supervision de la présente politique.

4.1.2 Approuve l'ensemble des rôles de sécurité, des responsabilités et des décisions de délégation.

4.1.3 Assure le suivi de la conformité et prend les décisions finales relatives aux dérogations à la politique et aux escalades.

4.2 Coordinateur sécurité désigné (le cas échéant)

4.2.1 Peut être un membre du personnel ou un consultant de confiance.

4.2.2 Ce rôle peut être assuré par le Directeur général ou par un prestataire externe dans les environnements de microentreprise.

4.2.3 Assiste au quotidien dans l'application du contrôle d'accès, la réponse aux incidents et les tâches techniques de sécurité de base.

4.2.4 Rend compte directement au Directeur général de tout problème ou risque de sécurité.