					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P02					Titre du document : **Politique relative aux rôles et responsabilités 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 5.3 ; Annexe A, contrôle 5	
ISO/IEC 27002:2022	Contrôle 5	
NIST SP 800-53 Rev.5	PL-1 à PL-4, PM-1 à PM-13	
RGPD de l'UE	Articles 5(1)(f), 24, 37	
NIS2 de l'UE	Article 21(2)(a)	
DORA de l'UE	Article 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Objet

1.1 La présente politique définit le modèle de gouvernance, les rôles organisationnels et les responsabilités nécessaires au fonctionnement efficace d'un système de management de la sécurité de l'information (SMSI).

1.2 Elle établit des responsabilités clairement définies, des pouvoirs de décision et des circuits d'escalade afin de garantir que la sécurité de l'information est intégrée à tous les niveaux de l'organisation et alignée sur les objectifs stratégiques de l'entreprise.

1.3 La présente politique met en œuvre les exigences de la clause 5.3 et du contrôle A.5.2 de l'ISO/IEC 27001:2022, en garantissant que les responsabilités relatives aux activités de sécurité sont clairement attribuées, documentées, communiquées et revues périodiquement.

1.4 La présente politique constitue également une base de gouvernance intégrée avec d'autres disciplines telles que la gestion des risques, la conformité, les opérations informatiques et les fonctions juridiques.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des personnes et entités participant à la gouvernance, à l'exploitation et à la supervision de la sécurité de l'information dans le périmètre du SMSI. Cela inclut :

2.1.1 la direction générale, l'encadrement supérieur et les membres du conseil d'administration ;

2.1.2 les responsables du SMSI, les RSSI et les responsables de contrôle ;

2.1.3 les responsables de processus et les propriétaires d'actifs ;

2.1.4 les prestataires et les fournisseurs tiers auxquels des responsabilités de sécurité ont été déléguées.

2.2 Elle couvre à la fois les fonctions internes et les fonctions externalisées (par exemple, un SOC externalisé ou des administrateurs de plateforme cloud) lorsque des rôles de gouvernance sont formellement attribués ou définis contractuellement.

2.3 La politique s'applique également aux unités organisationnelles, départements et équipes projet qui gèrent ou influencent des actifs, systèmes ou services pertinents au regard de la sécurité.

3. Objectifs

3.1 Garantir que les rôles et responsabilités en matière de sécurité de l'information sont formellement définis, attribués, communiqués et documentés.

3.2 Maintenir un modèle de gouvernance garantissant la séparation des tâches, éliminant les conflits d'intérêts et permettant l'escalade des sujets de sécurité non résolus.

3.3 Garantir que la responsabilité et l'autorité relatives aux décisions de sécurité sont réparties de manière cohérente avec l'impact métier et la structure organisationnelle.

3.4 Établir un cadre de gestion des délégations, des changements de rôle et de la revue des responsabilités attribuées.

3.5 Fournir aux parties prenantes — y compris les autorités de régulation, les auditeurs et les clients — l'assurance que la sécurité de l'information est gouvernée efficacement et conformément aux normes applicables.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Assure la supervision stratégique, alloue les ressources et veille à l'alignement entre les objectifs du SMSI et les objectifs de l'entreprise.

4.1.2 Approuve la documentation majeure du SMSI, y compris la Politique de sécurité de l'information, les plans de traitement des risques et les décisions de remédiation issues des audits.

4.1.3 Participe aux revues de direction du SMSI et porte en escalade les décisions nécessitant une approbation au niveau du conseil d'administration.

4.1.4 Porte une culture de la sécurité et promeut l'adhésion de l'organisation aux principes de gouvernance de la sécurité.

4.2 Comité de pilotage de la sécurité de l'information (ISSC)

4.2.1 Exerce le rôle d'instance de gouvernance transverse pour la supervision du SMSI.

4.2.2 Revoit l'exposition aux risques, la performance des contrôles, les constats d'audit et les initiatives stratégiques de sécurité.

4.2.3 Facilite la coordination entre les départements (par exemple, informatique, juridique, ressources humaines, risques, conformité, opérations).

4.2.4 Approuve les seuils d'escalade, les allocations budgétaires et les modifications de politique nécessitant un arbitrage de la direction.

[... 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

9.1.1 La présente politique doit faire l'objet d'une revue au moins annuelle ou lors de la survenance de l'un des événements suivants :

9.1.1.1 des changements de structure organisationnelle ou d'équipe dirigeante ;

9.1.1.2 une extension ou une redéfinition du périmètre du SMSI ;

9.1.1.3 des évolutions réglementaires affectant l'attribution des rôles ou la supervision ;

9.1.1.4 des constats d'audit significatifs ou des incidents impliquant une défaillance de gouvernance.

9.2 Processus de revue et d'approbation

9.2.1 Le responsable du SMSI doit initier et piloter le processus de revue, y compris la collecte des contributions des parties prenantes et des retours d'audit.

9.2.2 Les mises à jour proposées doivent être revues par l'ISSC et formellement approuvées par la direction générale.

9.2.3 Chaque version doit être suivie dans le registre documentaire du SMSI et inclure les métadonnées suivantes :

9.2.3.1 identifiant et titre de la politique ;

9.2.3.2 numéro de version et résumé des modifications ;

9.2.3.3 date d'entrée en vigueur et prochaine date de revue ;

9.2.3.4 propriétaire de la politique et approbateur ;

9.2.3.5 niveau de classification du document ;

9.2.3.6 historique de conservation et d'archivage.

10. Politiques associées et articulations

10.1 La présente politique doit être interprétée conjointement avec les politiques suivantes :

10.1.1 P1 – Politique de sécurité de l'information : établit le dispositif global de sécurité et définit les responsabilités de la direction en matière d'approbation des politiques et de supervision stratégique.

10.1.2 P5 – Politique de gestion des changements : garantit que les changements apportés aux structures de gouvernance, aux rôles ou aux responsabilités font l'objet d'une approbation documentée et d'une revue des risques.

10.1.3 P6 – Politique de gestion des risques : identifie et traite les risques de gouvernance résultant de conflits de rôles, de responsabilités non attribuées ou d'absence d'escalade.

10.1.4 P7 – Politique d'intégration et de départ : applique les processus d'attribution et de révocation des contrôles lors des changements intervenant dans le cycle de vie du personnel.

10.1.5 P33 – Politique de surveillance de l'audit et de la conformité : soutient la revue indépendante de l'efficacité de la gouvernance et impose des actions correctives en cas de non-conformité.

10.2 Ces politiques contribuent collectivement à un cadre de gouvernance du SMSI unifié et applicable.

11. Normes et référentiels de référence

11.1 La présente politique s'aligne sur des normes et référentiels mondialement reconnus en matière de gouvernance de la sécurité de l'information et d'attribution des responsabilités. Elle garantit la traçabilité vis-à-vis des exigences réglementaires et de certification, et soutient une structure de SMSI robuste et défendable.

11.2 ISO/IEC 27001

11.2.1 Clause 5.3 – Rôles, responsabilités et pouvoirs organisationnels : la présente politique satisfait à l'exigence selon laquelle les rôles pertinents pour la sécurité de l'information doivent être clairement attribués, communiqués et documentés.

11.2.2 Clause 9.3 – Revue de direction : la présente politique impose une supervision par la direction des rôles et de la gouvernance du SMSI au moyen de revues trimestrielles et annuelles.

11.2.3 Annexe A, contrôle 5.2 – Rôles et responsabilités en matière de sécurité de l'information : définit des rôles aux niveaux technique, opérationnel et stratégique afin d'assurer la séparation des tâches, le portage des risques et une responsabilité traçable.

11.3 ISO/IEC 27002:2022 – Contrôle 5

11.3.1 Fournit des recommandations de mise en œuvre pour l'attribution des responsabilités en matière de sécurité de l'information au sein d'une organisation. La présente politique reprend ces recommandations en définissant les types de rôles, les règles de délégation, les procédures d'escalade et les mécanismes de revue.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 à PL-4 : imposent la nécessité d'une documentation formelle de planification, y compris de politiques définissant la gouvernance et attribuant les responsabilités de sécurité.

11.4.2 PM-1 (plan du programme de sécurité de l'information) et PM-2 (responsable principal de la sécurité de l'information) : reflétés dans la présente politique par l'attribution du rôle de RSSI/responsable du SMSI et de rôles formels de gouvernance.

11.4.3 PM-5 à PM-13 : la présente politique satisfait aux exigences relatives à la documentation des rôles, aux rôles de gestion des risques à l'échelle de l'entreprise, à la supervision de la gestion de configuration et à l'intégration avec les fonctions métier et de mission.

11.5 RGPD de l'UE (2016/679)

11.5.1 Article 5(1)(f) : impose que les données à caractère personnel soient protégées contre tout traitement non autorisé ou illicite. La présente politique garantit que les personnes responsables de la protection des données sont clairement désignées et suivies.

11.5.2 Article 24 : exige des mesures organisationnelles appropriées, y compris des structures de gouvernance.

11.5.3 Article 37 : impose la désignation d'un délégué à la protection des données (DPO), qui doit être pris en compte dans le cadre de gouvernance de l'organisation et dans le registre des responsabilités.

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

11.6.1 Article 21(2)(a) : impose aux entités de mettre en œuvre des politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information, y compris des responsabilités propres à chaque rôle. La présente politique définit ces rôles et leurs mécanismes de gouvernance.

11.7 DORA de l'UE (2022/2554)

11.7.1 Article 5 – Gouvernance et cadre de contrôle interne : exige l'attribution formelle des responsabilités de gestion des risques liés aux TIC, des rôles décisionnels et des canaux de remontée d'information. La présente politique fournit la base de la gouvernance des rôles liés à la sécurité dans les environnements TIC.

11.8 COBIT 2019

11.8.1 EDM01 – Mise en place d'un cadre de gouvernance assuré : la présente politique garantit que le SMSI dispose d'une structure de gouvernance clairement définie et alignée sur les besoins de l'entreprise.

11.8.2 EDM02 – Réalisation des bénéfices assurée : aligne les activités de sécurité fondées sur les rôles avec les objectifs stratégiques et opérationnels, en garantissant responsabilité et résultats mesurables.

11.8.3 APO01 – Cadre de management de l'information et de la technologie géré et APO12 – Risque géré : la présente politique soutient une gestion structurée des rôles de sécurité de l'information dans un cadre plus large de gouvernance informatique et de gestion des risques.

11.8.4 MEA01 – Surveiller, évaluer et apprécier la performance : intègre des mécanismes de revue permettant de vérifier que les rôles de gouvernance sont efficaces, à jour et appliqués.