					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P06S					Titre du document : **Politique de gestion des risques**							
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 6.1, 6.1.3	
ISO/IEC 27002:2022	Mesures 5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 à RA-7, PM-9	
Directive NIS2 de l'UE	Article 21(2)(a–d)	
Règlement DORA de l'UE	Article 5	
COBIT 2019	APO12, MEA01	

1. Objet

1.1 La présente politique définit la manière dont l'organisation identifie, évalue et gère les risques liés à la sécurité de l'information, aux opérations, aux technologies et aux services fournis par des tiers.

1.2 Elle exige que la gestion des risques fasse partie intégrante de la planification, de l'exécution des projets, de la sélection des fournisseurs et de la réponse aux incidents, en cohérence avec l'ISO 27001, l'ISO 31000 et les exigences réglementaires.

1.3 La politique soutient une prise de décision éclairée, la protection des actifs informationnels et la résilience des activités essentielles.

2. Périmètre

2.1 La présente politique s'applique à :

2.1.1 Tous les services, systèmes et utilisateurs de l'organisation

2.1.2 Toutes les informations, tous les services et tous les actifs gérés en interne ou par des tiers

2.1.3 Toutes les activités liées aux risques, y compris les revues de projet, les mises à niveau des systèmes, l'externalisation et la conformité réglementaire

2.2 Elle couvre tous les types de risques, notamment :

2.2.1 Les menaces de cybersécurité et les vulnérabilités des systèmes

2.2.2 Les perturbations opérationnelles et les interruptions de service

2.2.3 Les expositions juridiques, de conformité ou réputationnelles

2.2.4 Les risques liés aux tiers et à la chaîne d'approvisionnement

2.3 Les employés et prestataires sont tenus de respecter la présente politique lors de l'identification ou du signalement des risques.

3. Objectifs

3.1 Intégrer des procédures d'évaluation des risques simples et reproductibles dans les opérations courantes.

3.2 Identifier et hiérarchiser les risques susceptibles d'affecter la confidentialité, l'intégrité, la disponibilité ou la conformité légale.

3.3 Attribuer un propriétaire et définir des actions de traitement pour tous les risques significatifs.

3.4 Tenir un registre des risques exact et à jour afin de faciliter le suivi des risques et la préparation des audits.

3.5 Assurer l'implication de la direction dans l'approbation de l'appétence au risque et des principaux plans de traitement.

4. Rôles et responsabilités

4.1 Directeur général

4.1.1 Définit l'appétence au risque de l'organisation et approuve le cadre de gestion des risques.

4.1.2 Approuve les principales décisions de traitement des risques ainsi que les ressources associées.

4.1.3 Passe en revue les principaux risques chaque trimestre avec le coordinateur des risques.

4.2 Coordinateur des risques (ou responsable du SMSI)

4.2.1 Facilite les évaluations des risques et tient à jour le registre des risques.

4.2.2 Veille à ce que la cotation des risques, la désignation des propriétaires et les actions de traitement soient documentées.

4.2.3 Organise au moins une revue formelle des risques par an.

[... 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 de la politique

9.1.1 La présente politique doit faire l'objet d'une revue au moins une fois par an par le Directeur général et le coordinateur des risques afin d'en garantir la pertinence et l'exhaustivité.

9.2 Déclencheurs de mise à jour

9.2.1 Une revue anticipée et une mise à jour doivent être engagées si :

9.2.1.1 Un incident majeur ou des constats d'audit mettent en évidence des lacunes dans la gestion des risques

9.2.1.2 De nouvelles unités d'activité, technologies ou partenariats sont introduits

9.2.1.3 Une exigence réglementaire ou contractuelle évolue

9.3 Gestion des versions

9.3.1 Toute mise à jour de la présente politique doit être versionnée avec les métadonnées suivantes :

9.3.1.1 Numéro de version et date d'entrée en vigueur

9.3.1.2 Synthèse des modifications

9.3.1.3 Approbateur (Directeur général)

9.3.1.4 Versions antérieures archivées à des fins d'audit

9.4 Communication et sensibilisation

9.4.1 Les versions mises à jour de la politique et les principaux plans de traitement des risques doivent être communiqués au personnel concerné. La sensibilisation annuelle doit inclure les principes fondamentaux de la sensibilisation aux risques.

10. Politiques associées et articulations

10.1 La présente politique s'articule avec plusieurs autres politiques afin d'assurer une gouvernance de la sécurité complète :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : définit les responsabilités en matière de propriété des risques et de prise de décision.

10.1.2 P5S – Politique de gestion des changements : impose une évaluation des risques avant la mise en œuvre de changements techniques ou procéduraux.

10.1.3 P17S – Politique de protection des données et de la vie privée : traite du risque réglementaire associé au traitement des données à caractère personnel.

10.1.4 P30S – Politique de réponse aux incidents : garantit la continuité du traitement des risques pendant et après les incidents de sécurité.

10.1.5 P33S – Politique de continuité d'activité : identifie les risques résiduels et les mesures de reprise applicables aux services critiques.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001 :

11.1.1 Clause 6.1 – Établit un processus formel de gestion des risques et de planification du traitement.

11.1.2 Clause 6.1.3 – Exige des organisations qu'elles conservent des plans de traitement documentés ainsi que les approbations associées.

11.2 ISO/IEC 27002 :

11.2.1 Mesures 5.4, 5.25 – Fournissent des orientations de mise en œuvre concernant la propriété des risques, la hiérarchisation et la gestion du cycle de vie.

11.3 NIST SP 800-53 Rev. 5 :

11.3.1 RA-1 à RA-7 – Définissent l'évaluation des risques, les stratégies de réponse, la documentation et les mécanismes de revue.

11.4 PM-9 – Exige une supervision cohérente, au niveau de la direction, des risques de l'organisation.

11.5 Directive NIS2 de l'UE

11.5.1 Article 21(2)(a–d) – Impose des contrôles obligatoires d'évaluation des risques, d'atténuation et de gouvernance aux entités essentielles et importantes.

11.6 Règlement DORA de l'UE

11.6.1 Article 5 – Exige des entités réglementées qu'elles définissent et gèrent des cadres de gestion des risques liés aux TIC, y compris l'identification, la classification et la réponse.

11.7 COBIT 2019

11.7.1 APO12 – Gérer les risques : intègre les risques dans la planification stratégique et opérationnelle.

11.7.2 MEA01 – Surveiller, évaluer et apprécier : assure l'efficacité et la conformité des processus et actions liés aux risques.