					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P01					Titre du document : **Politique de sécurité de l'information**							
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**

1. Objet

1.1 La présente politique formalise l'engagement global de l'organisation en matière de sécurité de l'information au travers de la mise en place d'un système de management de la sécurité de l'information (SMSI).

1.2 Elle définit l'orientation stratégique et les exigences fondamentales relatives à la protection de la confidentialité, de l'intégrité, de la disponibilité et de la résilience de l'ensemble des actifs informationnels, dans les environnements physiques, numériques et en cloud.

1.3 La présente politique répond aux exigences des clauses 5.1 et 5.2 de l'ISO/IEC 27001:2022 en exprimant l'intention de la direction, l'engagement de la direction générale et l'alignement des activités de sécurité sur les objectifs de l'organisation.

1.4 Elle constitue le document de référence à valeur d'autorité pour l'ensemble des politiques, normes et procédures subordonnées du SMSI et est indispensable à l'établissement d'un environnement de sécurité fondé sur les risques, orienté conformité et inscrit dans une démarche d'amélioration continue.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des personnes, actifs et processus définis dans le périmètre du SMSI, y compris :

2.1.1 Toutes les unités opérationnelles, tous les départements, toutes les filiales et toutes les succursales

2.1.2 Les salariés, prestataires, personnels temporaires, consultants et prestataires de services tiers

2.1.3 Toutes les données, tous les systèmes d'information, toutes les applications, toutes les infrastructures et tous les canaux de communication

2.1.4 Tous les environnements physiques, en cloud, distants et hybrides dans lesquels les données de l'entreprise sont traitées ou consultées

2.2 La présente politique s'impose à toute entité traitant des informations de l'organisation et couvre l'ensemble du cycle de vie de l'information, de sa création et de sa transmission jusqu'à son stockage et son élimination.

2.3 Toute exclusion ou limitation de ce périmètre doit être documentée dans la déclaration de périmètre du SMSI et justifiée par une approbation formelle de la direction générale.

3. Objectifs

3.1 Mettre en place un SMSI conforme à l'ISO/IEC 27001:2022 et apte à soutenir une prise de décision fondée sur les risques à l'échelle de l'entreprise.

3.2 Veiller à ce que les principes de confidentialité, d'intégrité et de disponibilité soient intégrés à l'ensemble des activités, systèmes et partenariats de l'organisation.

3.3 Assurer la conformité réglementaire et contractuelle en définissant des objectifs de sécurité mesurables, portés par la présente politique, et en les intégrant aux activités opérationnelles.

3.4 Réduire la probabilité et l'impact des incidents de sécurité de l'information au moyen de mesures préventives, de détection et correctives efficaces.

3.5 Renforcer en continu la maturité de l'organisation en matière de sécurité de l'information au moyen d'indicateurs de performance définis, des résultats d'audit et des revues de direction.

3.6 Promouvoir une culture de responsabilité, de sensibilisation et de résilience dans laquelle les responsabilités en matière de sécurité sont comprises et exercées par l'ensemble du personnel.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Approuve et soutient la politique de sécurité de l'information ainsi que le cadre du SMSI.

4.1.2 Veille à l’alignement entre les objectifs de sécurité et la stratégie de l’entreprise.

4.1.3 Donne l’impulsion et promeut une culture forte de la sécurité de l’information.

4.1.4 Examine et approuve les changements majeurs affectant le périmètre du SMSI, le traitement des risques et la structure de gouvernance.

4.2 Responsable de la sécurité des systèmes d’information (RSSI) / Responsable du SMSI

4.2.1 Est responsable du SMSI et maintient la présente politique en conformité avec l’ISO/IEC 27001.

4.2.2 Pilote les processus d’évaluation des risques, de mise en œuvre des mesures de sécurité et d’amélioration continue.

4.2.3 Assure la coordination transversale des actions de sécurité et supervise les politiques subordonnées.

4.2.4 Rend compte à la direction générale de l’état du SMSI, des incidents, des résultats d’audit et des indicateurs.

4.2.5 Veille à ce que les revues et mises à jour de la politique soient réalisées conformément à la section 9 du présent document.

[... 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 Fréquence de revue

9.1.1 La présente politique doit faire l’objet d’une revue au moins une fois par an ou en cas de survenance de l’un des événements suivants :

9.1.1.1 Modifications significatives des obligations légales, réglementaires ou contractuelles

9.1.1.2 Évolutions majeures du profil de risque de l’organisation

9.1.1.3 Résultats d’audits internes ou externes

9.1.1.4 Incidents majeurs ou défaillances de contrôle

9.2 Autorité et processus de revue

9.2.1 Le RSSI ou le responsable du SMSI désigné pilote le processus de revue.

9.2.2 Les éléments d’entrée de la revue doivent inclure :

9.2.2.1 Les résultats d’audit interne

9.2.2.2 Les tendances issues des évaluations des risques

9.2.2.3 Les évolutions des processus métier et des technologies

9.2.2.4 La performance au regard des indicateurs clés de performance et des seuils de risque

9.2.3 Toute mise à jour doit :

9.2.3.1 Être soumise au contrôle de version et documentée

9.2.3.2 Être approuvée par la direction générale

9.2.3.3 Être communiquée à toutes les parties concernées par les canaux officiels

9.2.3.4 Déclencher les mises à jour nécessaires de la documentation subordonnée et des formations

10. Politiques associées et articulations

10.1 Cette politique-cadre est directement articulée avec les politiques et référentiels de sécurité organisationnels suivants :

10.1.1 P2 – Politique relative aux rôles et responsabilités de gouvernance : définit la structure de gouvernance et la hiérarchie d’autorité visées dans le présent document.

10.1.2 P3 – Politique d'utilisation acceptable : encadre la conformité comportementale et l'utilisation appropriée des actifs informationnels.

10.1.3 P4 – Politique de contrôle d'accès : décline opérationnellement les contrôles liés à l'accès issus de la présente politique-cadre.

10.1.4 P6 – Politique de gestion des risques : fournit le cadre fondé sur les risques pour la sélection des contrôles et l'acceptation des risques résiduels.

10.1.5 P33 – Politique de surveillance d'audit et de conformité : décrit la manière dont les mécanismes internes d'assurance vérifient l'application de la politique.

10.2 Ces interdépendances garantissent un alignement complet et une traçabilité à l'échelle du SMSI, et soutiennent une gouvernance unifiée des risques et de la conformité.

11. Normes et référentiels de référence

11.1 La présente politique de sécurité de l'information est formellement alignée sur les normes et référentiels suivants afin d'assurer une conformité complète, une préparation à l'audit et la capacité de justifier le dispositif au regard des exigences réglementaires :

11.2 ISO/IEC 27001

11.2.1 Clause 5.1 – Leadership and Commitment : la présente politique démontre l'engagement de la direction générale en matière de sécurité de l'information et définit les responsabilités ainsi que l'allocation des ressources pour le SMSI.

11.2.2 Clause 5.2 – Information Security Policy : le présent document constitue la politique formelle de sécurité de l'organisation, alignée sur les objectifs de sécurité déclarés, la stratégie de l'entreprise et la conformité à l'ISO/IEC 27001.

11.2.3 Clause 6.1 – Actions to Address Risks and Opportunities : l'approche fondée sur les risques reflétée dans la présente politique garantit une allocation proportionnée des ressources de sécurité au regard des menaces.

11.2.4 Clause 9.2 – Internal Audit and Clause 10 – Improvement : la présente politique s'inscrit dans le cycle d'amélioration continue de l'organisation et fait l'objet d'une vérification dans le cadre de l'audit interne.

11.2.5 ISO/IEC 27002:2022 – Contrôle 5.1 : fournit des lignes directrices pour établir et maintenir des politiques de sécurité. La présente politique reprend les recommandations de l'ISO/IEC 27002 en matière de documentation hiérarchisée, de cycles de revue et de caractère opposable.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Security Planning Policy and Procedures) : la présente politique répond à l'exigence d'élaborer, de diffuser et de revoir une politique formelle de sécurité de l'information à l'échelle de l'organisation.

11.3.2 PM-1 à PM-5 : couvrent la gouvernance au niveau du programme, notamment les rôles en sécurité de l'information, l'allocation des ressources, la stratégie de risque et l'intégration de la planification de la sécurité dans les opérations de l'entreprise.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 5(2) : met en œuvre le principe de responsabilité. La présente politique définit les parties responsables et des actions d'application traçables.

11.4.2 Article 24 : impose la mise en œuvre de mesures techniques et organisationnelles, y compris de politiques alignées sur les risques.

11.4.3 Article 32 : soutient la mise en œuvre de mesures appropriées pour garantir la sécurité des données à caractère personnel tout au long de leur cycle de vie.

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

11.5.1 Article 21(2)(a) : impose aux entités de mettre en œuvre une politique de sécurité documentée couvrant la gestion des risques et la gouvernance. La présente politique répond à cette exigence et soutient plus largement l'état de préparation en cybersécurité ainsi que la protection des infrastructures critiques.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 5(2) : exige un cadre de contrôle interne documenté pour la gestion des risques liés aux TIC. La présente politique soutient la conformité du secteur financier en attribuant des rôles, des contrôles et des fonctions de supervision alignés sur les attentes de gouvernance de DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Governance Framework Setting : la présente politique soutient la gouvernance d'entreprise en définissant les rôles du SMSI, les engagements de la direction et les objectifs stratégiques.

11.7.2 APO01 – Management Framework : soutient la mise en place et le fonctionnement d'un SMSI structuré.

11.7.3 APO12 – Risk Management : fournit le fondement de la gouvernance des risques liés à la sécurité de l'information.

11.7.4 MEA01/MEA03 – Monitor, Evaluate and Assess : renforce l'évaluation continue de la performance et la surveillance du contrôle interne par l'application de la conformité à la politique.