					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P05					Titre du document : **Politique de gestion des changements**							
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 6.1, 5	Couvre les actions relatives aux risques, le contrôle d'accès et la gestion des changements
ISO/IEC 27002:2022	Mesure 8	Met en œuvre un processus structuré de gestion des changements
NIST SP 800-53 Rev.5	CM-2 à CM-14	Contrôles de gestion de la configuration
RGPD de l'UE	Articles 32(1)(b–d), 25 ; considérant 78	Mesures techniques et organisationnelles relatives à la sécurité des systèmes et des données pendant les changements
NIS2 de l'UE	Article 21(2)(a, b, d, e)	Implique la gestion des risques liés aux changements des TIC
DORA de l'UE	Articles 5, 8, 12	Encadre le risque opérationnel et le risque lié aux TIC, ainsi que la notification des incidents
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Gestion structurée des changements informatiques, performance, conformité et exigences

1. Objet

1.1. La présente politique établit un cadre formel pour l'initiation, l'évaluation, l'approbation, la mise en œuvre et la revue des changements apportés aux systèmes d'information, à l'infrastructure, aux applications et aux processus associés de l'organisation.

1.2. Elle impose que l'ensemble des changements soit exécuté de manière contrôlée et traçable à des fins d'audit, afin de réduire au minimum le risque de perturbation, de compromission de la sécurité ou de non-conformité réglementaire.

1.3. Elle soutient la mesure 8.32 de l'annexe A de l'ISO/IEC 27001:2022 en imposant des pratiques de gestion des changements sécurisées, documentées et alignées sur les risques.

1.4. La politique assure également la traçabilité des décisions relatives aux changements et renforce la résilience opérationnelle lors des modifications planifiées ou d'urgence.

2. Champ d'application

2.1. La présente politique s'applique à tous les changements affectant les systèmes, les données et les environnements relevant du périmètre d'application du SMSI, y compris :

2.1.1. l'infrastructure informatique (sur site, en cloud, hybride) ;

2.1.2. les environnements de production, de préproduction et de reprise après sinistre ;

2.1.3. les applications métier, les services, les interfaces de programmation applicative (API) et les intégrations ;

2.1.4. les paramètres de configuration, l'application des correctifs, les mises en production logicielles et les migrations de systèmes ;

2.1.5. les corrections d'urgence ainsi que les changements en mode projet ou planifiés.

2.2. Elle régit les changements initiés par :

2.2.1. le personnel interne (opérations informatiques, développeurs, propriétaires de systèmes) ;

2.2.2. les fournisseurs externes, les prestataires de services managés (MSP) et les prestataires de services ;

2.2.3. les équipes projet lors de la mise en œuvre de systèmes, de montées de version ou de transitions de services.

2.3. La présente politique ne s'applique pas :

2.3.1. aux environnements temporaires de test et de développement sans accès aux données de production ;

2.3.2. aux configurations personnelles des utilisateurs (couvertes par la Politique d'utilisation acceptable) ;

2.3.3. aux changements apportés à des systèmes situés hors du périmètre de contrôle de l'organisation, sauf s'ils affectent des actifs intégrés ou des obligations de conformité.

3. Objectifs

3.1. Garantir que tous les changements soient revus, approuvés, testés et documentés avant leur exécution.

3.2. Préserver la disponibilité des systèmes, l'intégrité des données et la continuité des services pendant et après les activités de changement.

3.3. Exiger des classifications de changement définies, des plans de retour arrière et des évaluations des risques pour tous les types de changement.

3.4. Permettre une prise de décision transparente et une escalade au moyen d'une gouvernance structurée.

3.5. Soutenir la préparation aux audits grâce à des enregistrements de changement traçables et à des revues après mise en œuvre.

3.6. Imposer la séparation des tâches et réduire le risque de changements non autorisés ou conflictuels dans les systèmes critiques.

4. Rôles et responsabilités

4.1. Haute direction

4.1.1. Approuve la Politique de gestion des changements et veille à son alignement sur les objectifs stratégiques et les obligations réglementaires.

4.1.2. Valide les programmes de changement à fort impact ou interfonctionnels dans le cadre de la supervision de la gouvernance.

4.1.3. Alloue les ressources et le budget nécessaires aux outils de contrôle des changements et à la formation du personnel.

4.2. Comité consultatif des changements

4.2.1. Revoit et autorise les changements standard et majeurs, en veillant à une évaluation appropriée des risques, des impacts et des dépendances.

4.2.2. Valide les plans de retour arrière, les résultats des tests, les communications aux parties prenantes et la planification.

4.2.3. Se compose des propriétaires de systèmes, de représentants de la sécurité, des opérations informatiques, des représentants métier et des représentants de la conformité.

4.2.4. Peut déléguer les décisions relatives aux changements à faible risque ou aux changements d’urgence dans des conditions documentées.

[... 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. Déclencheurs et fréquence de revue

9.1.1. La présente politique doit être revue annuellement ou à l’occasion de :

9.1.1.1. changements majeurs de l’informatique ou de l’infrastructure ;

9.1.1.2. incidents significatifs liés à des changements échoués ou non autorisés ;

9.1.1.3. mises à jour réglementaires ou nouvelles obligations juridiques liées aux changements ;

9.1.1.4. mise en œuvre de nouveaux outils ou de nouvelles plateformes CMS.

9.2. Processus de revue de la Politique de gestion des changements

9.2.1. Le Responsable de la gestion des changements pilote le processus de revue en collaboration avec :

9.2.1.1. l’informatique, la sécurité et les opérations ;

9.2.1.2. l’audit interne et les risques ;

9.2.1.3. les représentants du Comité consultatif des changements.

9.2.2. Les mises à jour doivent être revues et approuvées par la haute direction et le comité de pilotage du SMSI.

9.2.3. Les versions réémises doivent faire l’objet d’un suivi dans le registre documentaire et être communiquées aux parties concernées avec une nouvelle prise de connaissance lorsque nécessaire.

9.3. Contrôle documentaire et gestion des versions

9.3.1. Toutes les versions doivent inclure :

9.3.1.1. l’identifiant de la politique, le titre et le niveau de classification ;

9.3.1.2. le propriétaire et l’historique des révisions ;

9.3.1.3. le journal des modifications et la date d’entrée en vigueur ;

9.3.1.4. l’autorité d’approbation.

9.3.2. Les versions archivées doivent être conservées conformément à la Politique de conservation des documents (minimum 3 ans).

10. Politiques associées et articulations

10.1. La présente politique est directement articulée avec les documents suivants et en soutient l’application :

10.1.1. P1 – Politique de sécurité de l'information : établit l’exigence de contrôles de sécurité formels et de responsabilisation au niveau des processus, y compris la gouvernance de la gestion des changements.

10.1.2. P2 – Politique relative aux rôles et responsabilités de gouvernance : définit les autorités d’approbation et la séparation des tâches applicables à l’autorisation et à la supervision des changements.

10.1.3. P4 – Politique de contrôle d’accès : veille à ce que les autorisations d’accès des personnes mettant en œuvre et revoyant les changements respectent le principe du moindre privilège.

10.1.4. P6 – Politique de gestion des risques : veille à ce que tous les changements fassent l’objet d’une évaluation des risques appropriée et de stratégies d’atténuation adaptées.

10.1.5. P33 – Politique de surveillance de l'audit et de la conformité : régit la validation et la revue d'audit des enregistrements et des manquements liés à la gestion des changements.

10.2. Ensemble, ces politiques permettent un cycle de vie de gestion des changements au sein du cadre du SMSI qui soit défendable, traçable et sécurisé.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001:2022

11.1.1. Article 6.1 – Actions visant à traiter les risques et opportunités : la présente politique soutient l'identification, l'évaluation et la maîtrise des risques liés aux changements.

11.1.2. Article 5.15 – Contrôle d'accès : veille à ce que les accès pendant les changements soient contrôlés et traçables.

11.1.3. Annexe A, mesure 8.32 – Gestion des changements : la présente politique met pleinement en œuvre l'exigence de gestion planifiée et contrôlée des changements apportés aux moyens de traitement de l'information et aux systèmes.

11.2. ISO/IEC 27002:2022 – Mesure 8

11.2.1. Renforce la mise en œuvre d'un processus structuré de gestion des changements, incluant la classification des changements, l'approbation, les tests, le retour arrière et la documentation.

11.3. NIST SP 800-53 Rev.5

11.3.1. Famille CM (CM-1 à CM-14) : la présente politique est étroitement alignée sur les contrôles de gestion de la configuration, y compris les configurations de référence (CM-2), le contrôle des changements de configuration (CM-3), l'analyse d'impact sur la sécurité (CM-4) et les restrictions d'accès (CM-5).

11.3.2. Famille AU (AU-2, AU-6, AU-12) : les mécanismes de journalisation et d'audit référencés dans la présente politique soutiennent la traçabilité des événements et la revue de conformité des activités liées aux changements.

11.3.3. RA-3, RA-5 : les évaluations des risques induites par les changements et les scans de vulnérabilités sont intégrés au processus d'évaluation des changements.

11.3.4. PM-11 (Définition de la mission / des processus métier) : veille à ce que la continuité d'activité et les objectifs opérationnels soient préservés pendant les changements.

11.4. RGPD de l'UE (2016/679)

11.4.1. Article 32(1)(b–d) : la présente politique soutient l'exigence de mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, en particulier lors des changements de système.

11.4.2. Article 25 – Protection des données dès la conception et par défaut : veille à ce que les changements affectant les données à caractère personnel intègrent la protection de la vie privée et la sécurité dans la conception et le déploiement.

11.4.3. Considérant 78 : exige que les responsables du traitement mettent en œuvre des mécanismes, tels que des politiques de contrôle des changements, afin d'assurer la confidentialité, l'intégrité et la résilience continues des systèmes de traitement.

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

11.5.1. Article 21(2)(a, b, d, e) : impose des mesures techniques et organisationnelles pour gérer les risques liés aux TIC, y compris ceux résultant des changements système, des mises à jour logicielles et des modifications d'infrastructure.

11.6. DORA de l'UE (2022/2554)

11.6.1. Article 5 – Cadre de gouvernance et de contrôle interne : la présente politique impose des principes de gestion des risques opérationnels liés aux changements et aux mises à jour des TIC.

11.6.2. Article 8 – Cadre de gestion des risques liés aux TIC : impose aux entités financières de gérer tous les changements affectant les systèmes TIC dans le cadre de processus structurés de gestion des changements, ce qui se reflète dans les exigences de classification, de test, de retour arrière et de documentation de la présente politique.

11.6.3. Article 12 – Notification des incidents : veille à ce que les changements défaillants entraînant des perturbations des TIC soient traçables, documentés et notifiés lorsque cela est applicable.

11.7. COBIT 2019

11.7.1. BAI06 – Gestion des changements informatiques : la présente politique répond directement aux objectifs de BAI06 en établissant des flux de travail structurés pour l'approbation des changements, l'évaluation des impacts, la communication et les tests.

11.7.2. BAI02 – Gestion de la définition des exigences et BAI03 – Gestion de l'identification et de la construction des solutions : veillent à ce que les changements motivés par l'activité soient revus et mis en œuvre de manière sécurisée.

11.7.3. DSS01 – Gestion des opérations : soutient l'intégrité continue des systèmes pendant l'exécution des changements.

11.7.4. MEA01 et MEA03 – Surveiller, évaluer et apprécier la performance et la conformité : permet une supervision continue de l'efficacité et de l'application de la politique de gestion des changements.