					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P05S					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, 8	
ISO/IEC 27002:2022	Mesure 8	
NIST SP 800-53 Rev.5	CM-2 à CM-5, CM-11	
NIS2 (UE)	Article 21(2)(b)	
DORA (UE)	Articles 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Objet

1.1 La présente politique impose que toute modification apportée aux systèmes informatiques, aux configurations, aux applications métier ou aux services cloud soit planifiée, évaluée au regard des risques, testée et approuvée avant sa mise en œuvre.

1.2 Elle vise à réduire les perturbations opérationnelles, les risques de sécurité et les interruptions de service en définissant un processus simplifié mais formalisé, également applicable aux petites entreprises disposant de ressources limitées.

1.3 La présente politique contribue à la certification ISO/IEC 27001:2022 en formalisant la manière dont les changements techniques et opérationnels sont gérés et documentés.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 aux employés et responsables de service qui proposent ou mettent en œuvre des changements

2.1.2 aux prestataires externes de services informatiques qui administrent des systèmes ou des logiciels

2.1.3 au directeur général, qui assume la responsabilité globale des approbations de changement

2.2 Elle couvre les changements portant sur :

2.2.1 les logiciels (mises à jour, correctifs, nouvelles applications)

2.2.2 le matériel (remplacements, montées de version)

2.2.3 les configurations réseau et de pare-feu

2.2.4 les services cloud, les droits d'accès des utilisateurs ou les intégrations avec des fournisseurs

2.2.5 les changements critiques de processus métier impliquant des systèmes d'information

2.3 Les changements planifiés comme les changements d'urgence relèvent du champ d'application de la présente politique.

3. Objectifs

3.1 Garantir que tous les changements affectant l'informatique et les systèmes métier sont autorisés, documentés et réversibles en cas de problème.

3.2 Prévenir les indisponibilités non planifiées, les pertes de données ou les incidents de sécurité causés par des changements non maîtrisés.

3.3 Définir des procédures simples et reproductibles pour la soumission, l'approbation, les tests et le retour arrière des changements.

3.4 Tenir un journal des changements exploitable en audit afin d'assurer la traçabilité des responsabilités opérationnelles et la conformité réglementaire.

3.5 Permettre une prise de décision fondée sur les risques pour les changements significatifs ou sensibles.

4. Rôles et responsabilités

4.1 Directeur général

4.1.1 Assume la responsabilité finale de l'ensemble des changements majeurs.

4.1.2 Examine et approuve les changements non courants, critiques ou à risque élevé.

4.1.3 Passe en revue le journal des changements chaque trimestre ou à la suite d'incidents majeurs.

4.2 Support informatique ou prestataire informatique externalisé

4.2.1 Met en œuvre les changements, y compris les mises à jour de configuration, l'application de correctifs et les migrations de systèmes.

4.2.2 Tient un journal des changements de base consignant les dates, les types de changement, les résultats et les approbateurs.

4.2.3 Teste les changements avant leur mise en œuvre et applique les procédures de retour arrière si nécessaire.

4.2.4 Informe les utilisateurs concernés avant et après les changements majeurs.

[... 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

9.1.1 La présente politique doit faire l'objet d'une revue annuelle par le directeur général ou le référent informatique désigné afin de garantir son alignement avec les systèmes, les processus de travail et les exigences réglementaires en vigueur.

9.2 Revues intermédiaires

9.2.1 Des revues doivent également être déclenchées dans les cas suivants :

9.2.1.1 incidents de sécurité causés par une mauvaise gestion des changements

9.2.1.2 introduction de nouveaux systèmes informatiques

9.2.1.3 évolutions des normes pertinentes telles que l'ISO, NIS2 ou DORA

9.3 Documentation des mises à jour

9.3.1 Les modifications apportées à la présente politique doivent faire l'objet d'un contrôle de version et être approuvées par le directeur général. Chaque version doit mentionner la date, le résumé des modifications et l'approbateur.

9.4 Communication de la politique

9.4.1 Toute mise à jour doit être communiquée à l'ensemble des employés et prestataires externes concernés. La documentation doit être mise à jour dans tous les emplacements de référence (par exemple, portail du personnel, lecteurs partagés).

10. Politiques connexes et articulations

10.1 La présente politique est étroitement liée aux politiques PME suivantes :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : définit l'autorité d'approbation des changements.

10.1.2 P4S – Politique de contrôle d'accès : garantit que les modifications d'accès résultant de changements sont documentées et mises en œuvre correctement.

10.1.3 P7S – Politique d'intégration et de départ : coordonne les changements liés aux transitions de rôle et à l'attribution des accès.

10.1.4 P15S – Politique de sauvegarde et de restauration : garantit que les étapes de retour arrière et de reprise peuvent être exécutées en cas d'échec d'un changement.

10.1.5 P30S – Politique de réponse aux incidents : encadre le traitement des changements échoués ou non autorisés en tant qu'incidents de sécurité.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 6.1 – La planification fondée sur les risques doit inclure les activités de changement.

11.1.2 Article 8.1 – Des contrôles opérationnels doivent être appliqués de manière cohérente aux activités liées aux changements afin de garantir l'intégrité du service.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.32 – Fournit des lignes directrices pour des processus sécurisés de gestion des changements, y compris la documentation, les tests et l'approbation.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-2 – Configuration de référence des systèmes avant changement.

11.3.2 CM-3 – Contrôle des changements de configuration.

11.3.3 CM-4 – Analyse d'impact sur la sécurité.

11.3.4 CM-5 – Approbation et documentation des changements.

11.3.5 CM-11 – Audit et surveillance des changements.

11.4 Directive NIS2 (UE)

11.4.1 Article 21(2)(b) – Exige des procédures formalisées pour les mesures de sécurité techniques et organisationnelles, y compris la gestion des changements.

11.5 DORA (UE)

11.5.1 Articles 6(9) et 8(4)(b) – Exigent des entités financières qu'elles maintiennent une gestion des changements et des configurations pour les systèmes TIC.

11.6 COBIT 2019

11.6.1 BAI06 – Gérer les changements : met l'accent sur la planification, l'évaluation des risques et les capacités de retour arrière.

11.6.2 DSS01 – Gérer les opérations : garantit l'intégrité opérationnelle lors des transitions et changements techniques.