					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P15S					Titre du document : **Politique de sauvegarde et de restauration**							
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 avec les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clause 8	Mesures de sauvegarde conformes aux exigences du SMSI
ISO/IEC 27002:2022	Mesures 5.29, 8.13	Bonnes pratiques de sauvegarde et intégration à la continuité d'activité
NIST SP 800-53 Rev.5	CP-9, MP-6	Sauvegarde et protection des supports
Directive NIS2 de l'UE	Article 21(2)(c)	Résilience et continuité assurées au moyen de sauvegardes
Règlement DORA de l'UE	Article 10(1)	Continuité des TIC - sauvegardes pour les entités financières
COBIT 2019	BAI04.05, DSS04	Documentation et tests des sauvegardes, maîtrise des processus
RGPD	Articles 5(1)(f), 32(1)(c)	Intégrité, disponibilité et restauration rapide des données

1. Objet

1.1 La présente politique définit la manière dont l'organisation met en œuvre et gère les sauvegardes afin d'assurer la continuité d'activité, de se prémunir contre la perte de données et de permettre un rétablissement rapide après incident.

1.2 Elle établit des règles contraignantes relatives à la sauvegarde, au stockage et à la restauration des systèmes et des données, en particulier dans les PME ne disposant pas d'une infrastructure informatique complexe.

1.3 Cette politique contribue à la préparation aux audits et à la certification ISO/IEC 27001 en garantissant que les mesures de sauvegarde essentielles sont en place, appliquées de manière cohérente et revues régulièrement.

1.4 La capacité de l'organisation à se rétablir après des défaillances techniques, une suppression accidentelle ou des incidents cyber dépend du respect strict de la présente politique.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des systèmes métier et des données, y compris :

2.1.1 les enregistrements financiers, les informations clients et les données RH ;

2.1.2 les postes de travail fixes, les ordinateurs portables, les serveurs et les applications cloud utilisés dans le cadre des opérations de l'entreprise ;

2.1.3 les supports de sauvegarde tels que les clés USB, les supports de stockage externes ou les sauvegardes cloud.

2.2 Elle s'applique également à toute personne ayant une responsabilité dans l'exécution ou la gestion des processus de sauvegarde, notamment :

2.2.1 le Directeur général (DG) ou la personne responsable désignée ;

2.2.2 les prestataires externes de support informatique ou les consultants ;

2.2.3 tous les employés chargés d'enregistrer les données dans des emplacements approuvés.

3. Objectifs

3.1 Garantir que toutes les données et tous les systèmes critiques pour l'activité sont sauvegardés de manière sécurisée à des intervalles appropriés, en fonction du risque et des besoins opérationnels.

3.2 Garantir que les données peuvent être restaurées de manière complète dans des délais appropriés à la suite d'une perturbation.

3.3 Prévenir tout accès non autorisé, toute altération ou toute perte des données de sauvegarde au moyen de contrôles de stockage efficaces.

3.4 Définir clairement et appliquer les rôles et responsabilités relatifs à la mise en œuvre et aux tests des procédures de sauvegarde.

3.5 Soutenir la conformité à l'ISO/IEC 27001, au RGPD et aux autres obligations réglementaires au moyen de pratiques de sauvegarde structurées et documentées.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve la présente politique et veille à son application.

4.1.2 Alloue les ressources et désigne les responsabilités relatives aux activités de sauvegarde et de restauration.

4.1.3 Examine les échecs de sauvegarde, les incidents et les écarts à la politique.

4.1.4 Dirige les revues annuelles de la politique et veille à la préparation aux audits.

4.2 Prestataire externe de support informatique (le cas échéant)

4.2.1 Met en œuvre et gère les solutions de sauvegarde, qu'elles soient locales ou cloud.

4.2.2 Assure le suivi du bon déroulement des sauvegardes et planifie les tests de restauration.

4.2.3 Signale directement au DG les défaillances et les incidents.

4.2.4 Veille au chiffrement, aux restrictions d'accès et au traitement approprié des supports de sauvegarde.

[... 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 La présente politique doit être revue au moins une fois par an par le DG. Les déclencheurs de revue intermédiaire incluent :

9.1.1 des changements majeurs dans les systèmes ou les méthodes de stockage ;

9.1.2 l'introduction de nouvelles plateformes cloud ou de nouvelles plateformes informatiques ;

9.1.3 des évolutions juridiques ou réglementaires affectant la restauration des données ;

9.1.4 des constats issus d'audits ou d'incidents.

9.2 Le DG est responsable du lancement de la revue, de l'approbation des changements et de la communication des mises à jour.

9.3 Les versions de la politique doivent faire l'objet d'un suivi et d'un archivage. Les versions remplacées doivent être soumises à des restrictions d'accès afin d'éviter toute confusion lors des audits ou des opérations de reprise d'activité.

10. Politiques associées et articulations

10.1 La présente politique est alignée sur les politiques SME suivantes et s'articule avec elles :

10.1.1 P14S – Politique de conservation et d'élimination des données : définit la durée de conservation des données de sauvegarde et les modalités de leur suppression sécurisée.

10.1.2 P13S – Politique de classification et d'étiquetage des données : aide à prioriser les données devant être sauvegardées selon leur niveau de classification.

10.1.3 P30S – Politique de réponse aux incidents : couvre les procédures applicables en cas d'échec de sauvegarde ou lorsque la restauration des données est requise après une violation ou une interruption de service.

10.1.4 P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue une autorité claire pour la supervision des sauvegardes et l'application de la politique.

10.1.5 P17S – Politique de protection des données et de la vie privée : garantit que le traitement des données à caractère personnel dans le cadre des sauvegardes est conforme aux exigences légales et de protection de la vie privée.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 : planification et contrôle opérationnels des systèmes de sauvegarde dans le cadre du SMSI.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.13 : prescrit les bonnes pratiques relatives à la planification, à la surveillance et à la restauration des sauvegardes.

11.2.2 Annexe A, mesure 5.29 : intégration des sauvegardes à la continuité d'activité et à l'aptitude à la restauration.

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Contingency Planning) : définit des stratégies de sauvegarde structurées pour la résilience de l'activité.

11.3.2 MP-6 (Media Protection) : impose le traitement sécurisé et la destruction des supports de sauvegarde.

11.4 RGPD

11.4.1 Article 5(1)(f) : impose l'intégrité et la disponibilité des données à caractère personnel.

11.4.2 Article 32(1)(c) : impose la capacité de rétablir l'accès aux données à caractère personnel dans des délais appropriés.

11.5 Directive NIS2 de l'UE

11.5.1 Article 21(2)(c) : impose la sauvegarde et la restauration dans le cadre de la planification de la résilience et de la continuité.

11.6 Règlement DORA de l'UE

11.6.1 Article 10(1) : les organisations du secteur financier doivent assurer des sauvegardes dans le cadre des mesures de continuité des TIC.

11.7 COBIT 2019

11.7.1 BAI04.05 : impose des stratégies de sauvegarde documentées.

11.7.2 DSS04.07 : met l'accent sur les tests réguliers et la maîtrise des processus de sauvegarde et de restauration des données.