					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P15					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 sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clauses 6.1.3, 8	Traitement des risques, planification et contrôles opérationnels de sauvegarde
ISO/IEC 27002:2022	Mesures 8.13, 5.28, 5.29	Gestion des sauvegardes, élimination sécurisée et résilience
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Exigences relatives à la sauvegarde des systèmes, au rétablissement et à l'assainissement des supports
RGPD de l'UE	Article 32, considérant 49	Restauration et disponibilité des données à caractère personnel, continuité d'activité
NIS2 de l'UE	Article 21(2)(c-e)	Contrôles de sauvegarde et de continuité pour la résilience
DORA de l'UE	Articles 10, 11	Exigences du secteur financier en matière de sauvegarde, de rétablissement et de tests
COBIT 2019	DSS01, DSS04, MEA03	Opérations de sauvegarde, continuité et surveillance de la conformité

1. Objet

1.1 La présente politique a pour objet de définir les exigences obligatoires relatives à la sauvegarde et à la restauration des données, des systèmes et des applications afin de soutenir la résilience opérationnelle, l'intégrité des données et la continuité d'activité.

1.2 La politique établit un cadre normalisé visant à :

1.2.1 Protéger les données de l'organisation contre les pertes dues à la suppression, à la corruption, à une défaillance ou à des cyberattaques

1.2.2 Définir les attentes de rétablissement au moyen de paramètres clairs de RTO (Recovery Time Objective) et de RPO (Recovery Point Objective)

1.2.3 Intégrer les opérations de sauvegarde au cadre plus large du SMSI et aux plans de continuité d'activité et de reprise après sinistre (BCP/DRP)

1.2.4 Garantir la conformité aux lois applicables et aux réglementations sectorielles relatives à la disponibilité et à la capacité de restauration

1.3 La politique met en œuvre les mesures de l'ISO/IEC 27001:2022 relatives à l'élimination sécurisée des données (5.28), à la résilience (5.29) et au rétablissement opérationnel (8.13), et s'aligne sur les bonnes pratiques d'ISO/IEC 27002:2022, de NIST SP 800-53 Rev.5, du RGPD, de DORA et de NIS2.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les systèmes critiques pour l'activité et les systèmes opérationnels relevant du domaine d'application du SMSI

2.1.2 Toutes les données métier structurées et non structurées, y compris les bases de données, fichiers, courriels et configurations

2.1.3 Tous les environnements — sur site, cloud, hybrides et stockage distant/hors site

2.1.4 L'ensemble du personnel chargé de gérer, d'exécuter, de vérifier ou de restaurer les processus de sauvegarde

2.2 Elle s'applique également à :

2.2.1 L'infrastructure et les supports de sauvegarde, y compris les bandes physiques, appliances virtuelles, instantanés de disque et solutions de sauvegarde fondées sur le cloud

2.2.2 Les prestataires tiers mandatés pour héberger, gérer ou traiter les sauvegardes de l'organisation

2.2.3 La sauvegarde des journaux, des configurations, des pistes d'audit et de la documentation opérationnelle essentielle à la continuité

2.3 Les systèmes explicitement exclus de la sauvegarde doivent être documentés, faire l'objet d'une évaluation des risques et être formellement approuvés par le responsable du SMSI et le propriétaire du système.

3. Objectifs

3.1 Garantir que tous les systèmes et données critiques font l'objet de sauvegardes fiables, avec une fréquence, une redondance et des mesures de sécurité suffisantes.

3.2 Prévoir des mécanismes de restauration permettant de respecter les objectifs RTO et RPO définis, en cohérence avec les analyses d'impact sur l'activité.

3.3 Maintenir une documentation complète des procédures de sauvegarde, des calendriers de conservation, des rôles et des technologies.

3.4 Valider l'efficacité des opérations de sauvegarde au moyen de tests systématiques de restauration, de la journalisation des échecs et du suivi des actions correctives.

3.5 Protéger les données de sauvegarde contre tout accès non autorisé, toute modification ou destruction tout au long de leur cycle de vie.

3.6 Assurer la conformité avec :

3.6.1 Les exigences d'ISO/IEC 27001 en matière de contrôles opérationnels et de continuité

3.6.2 Les familles CP et MP de NIST SP 800-53 relatives à la sauvegarde et à l'assainissement

3.6.3 L'article 32 et le considérant 49 du RGPD concernant la restauration de l'accès aux données à caractère personnel

3.6.4 L'article 10 de DORA et l'article 21 de NIS2 concernant la continuité et la résilience des TIC

3.7 Garantir que les services de sauvegarde fournis par des tiers respectent les obligations contractuelles et réglementaires en matière de sécurité, y compris le chiffrement, l'élimination et les protocoles de notification.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve la présente politique et veille à ce que les systèmes critiques pour l'activité soient protégés de manière adéquate par des pratiques de sauvegarde et de restauration approuvées.

4.1.2 S'assure que les opérations de sauvegarde disposent de ressources suffisantes et fassent l'objet d'une revue périodique au regard de la conformité réglementaire.

4.2 Responsable de la sécurité des systèmes d'information (RSSI)

4.2.1 Est responsable de la présente politique et veille à son alignement avec les cadres plus larges de sécurité de l'information, de gestion des risques et de continuité.

4.2.2 Supervise l’intégration des procédures de sauvegarde dans les plans de continuité d’activité et de reprise après sinistre (BCP/DRP), la réponse aux incidents et la planification de la résilience.

4.2.3 Examine les dérogations relatives aux sauvegardes et évalue les propositions d’acceptation du risque concernant les exclusions de systèmes critiques.

[... 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 faire l’objet d’une revue au moins une fois par an, ou plus tôt en cas de déclenchement par :

9.1.1 Des changements dans la stratégie de continuité d’activité ou de reprise après sinistre

9.1.2 De nouvelles obligations réglementaires ou légales ayant une incidence sur la fréquence des sauvegardes ou la conservation des données

9.1.3 Des changements dans l’architecture des systèmes, les outils de sauvegarde ou les prestataires de services

9.1.4 Des incidents significatifs ou des constats d’audit liés à une perte de données ou à des échecs de rétablissement

9.2 La revue doit être coordonnée par le RSSI en collaboration avec :

9.2.1 Les équipes Infrastructure et Exploitation informatique

9.2.2 L’audit interne

9.2.3 Le Délégué à la protection des données (DPO)

9.2.4 Les équipes de continuité d’activité et de reprise après sinistre

9.3 Les calendriers de sauvegarde, les listes des systèmes inclus, la documentation de restauration et les journaux d’exception doivent être revus en parallèle afin de garantir :

9.3.1 L’exactitude de la couverture des sauvegardes pour tous les actifs critiques

9.3.2 La conformité aux exigences RTO/RPO et de conservation

9.3.3 L’exhaustivité des journaux de test et des rapports d’incident

9.3.4 La correction des lacunes de contrôle précédemment identifiées

9.4 Toute mise à jour doit :

9.4.1 Être gérée selon la gestion des versions et conservée dans le référentiel documentaire du SMSI

9.4.2 Inclure un résumé des modifications et leur justification

9.4.3 Être approuvée par la haute direction

9.4.4 Être communiquée à l’ensemble du personnel technique et métier concerné

10. Politiques associées et articulations

10.1 La présente politique soutient directement les documents associés ci-dessous et s’articule avec eux :

10.1.1 P6 - Politique de gestion des risques : identifie la priorisation fondée sur les risques de la protection par sauvegarde des systèmes et services.

10.1.2 P12 - Politique de gestion des actifs : garantit que les systèmes éligibles à la sauvegarde sont recensés dans l’inventaire et rattachés au suivi du cycle de vie et à la classification.

10.1.3 P13 - Politique de classification et d’étiquetage des données : précise quelles catégories de données doivent être sauvegardées, y compris les métadonnées d’étiquetage utilisées pour la priorisation.

10.1.4 P14 - Politique de conservation et d'élimination des données : coordonne la conservation des sauvegardes avec les limites réglementaires de conservation et l'élimination appropriée des supports arrivés à expiration.

10.1.5 P16 - Politique de masquage des données et de pseudonymisation : soutient la minimisation des données lors de la sauvegarde d'ensembles de données sensibles.

10.1.6 P30 - Politique de réponse aux incidents : activée en cas d'échec de sauvegarde, de problème de restauration ou de compromission des dépôts de sauvegarde.

10.2 Ces politiques interconnectées forment un cadre cohérent garantissant que la gouvernance des sauvegardes est intégrée au cadre plus large du SMSI et à la stratégie de résilience opérationnelle de l'organisation.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001:

11.1.1 Clause 6.1.3 - Plan de traitement des risques : soutient la priorisation des sauvegardes fondée sur les risques et la planification de la restauration.

11.1.2 Clause 8.1 - Planification et contrôle opérationnels : intègre les contrôles de rétablissement et de continuité dans les mesures de protection opérationnelles.

11.1.3 Annexe A Mesure 5.28 - Élimination sécurisée ou réutilisation des équipements : traite de l'assainissement sécurisé des supports de sauvegarde.

11.1.4 Annexe A Mesure 5.29 - Sécurité de l'information en situation de perturbation : garantit les capacités de restauration lors d'incidents ou de sinistres.

11.1.5 Annexe A Mesure 8.13 - Sauvegarde des informations : traitée directement au moyen d'opérations de sauvegarde planifiées, testées et sécurisées.

11.2 ISO/IEC 27002:2022 - Mesures 8.13, 5.28, 5.29 : ces mesures renforcent l'exigence de sauvegardes régulières, de validation de l'intégrité et de planification de la restauration dans tous les environnements informatiques.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Sauvegarde du système : établit des procédures complètes de sauvegarde, y compris le stockage hors site et les tests de restauration.

11.3.2 CP-10 - Récupération et restauration du système : exige des procédures validées de restauration complète ou partielle alignées sur les objectifs de rétablissement.

11.3.3 MP-6 - Assainissement des supports : garantit le traitement sécurisé des supports de sauvegarde obsolètes.

11.3.4 SI-12 - Procédures de traitement de l'information : renforce les responsabilités en matière de sauvegarde et de rétablissement pour les données sensibles.

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

11.4.1 Article 32 - Sécurité du traitement : impose des capacités de restauration et des mesures de protection de la disponibilité des données, notamment pour les données à caractère personnel.

11.4.2 Considérant 49 : soutient les mesures de continuité d'activité et de reprise après sinistre, y compris la sauvegarde sécurisée en tant qu'élément de la résilience organisationnelle.

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

11.5.1 Article 21(2)(c-e) : exige des mesures techniques et organisationnelles, y compris des contrôles de sauvegarde et de continuité, afin d'assurer la résilience des services.

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

11.6.1 Article 10 - Continuité d’activité des TIC : exige des entités financières qu’elles disposent d’une sauvegarde complète des données, de capacités de rétablissement et d’une planification de continuité.

11.6.2 Article 11 - Tests des plans de continuité d’activité des TIC : met l’accent sur la validation des capacités de rétablissement par des tests réguliers.

11.7 COBIT 2019:

11.7.1 DSS01 - Gestion des opérations : soutient une fourniture fiable des services grâce à une disponibilité protégée des données.

11.7.2 DSS04 - Gestion de la continuité : définit les contrôles stratégiques et opérationnels de continuité, y compris les sauvegardes vérifiées.

11.7.3 MEA03 - Surveiller, évaluer et apprécier la conformité : impose une revue périodique des mesures de continuité, y compris l’efficacité des contrôles de sauvegarde.