					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P14S					Titre du document : **Politique de conservation et d'élimination des données**							
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 6.1.3, 8	Couvre le traitement des risques, les contrôles opérationnels et les exigences de conservation
ISO/IEC 27002:2022	Mesure 5	Fournit des lignes directrices sur les durées de conservation et les méthodes de destruction sécurisée
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Conservation des journaux d'audit, assainissement des supports, limites de conservation des données et mise en application
NIS2	Article 21(2)(a)	Politique de gestion du cycle de vie adaptée au risque requise
DORA	Article 5(1)	Gestion des risques liés aux TIC : disponibilité et suppression des données
COBIT 2019	BAI03.04, DSS01	Contrôles du cycle de vie de l'information, élimination sécurisée
RGPD	Article 5(1)(e), 17	Les données ne doivent pas être conservées plus longtemps que nécessaire ; droit à l'effacement

1. Objet

1.1 La présente politique a pour objet de définir des règles contraignantes en matière de conservation et d'élimination sécurisée des informations dans un environnement de PME. Elle impose que les enregistrements ne soient conservés que pendant la durée requise par la loi, une obligation contractuelle ou un besoin métier, puis détruits de manière sécurisée.

1.2 Cette politique vise à réduire le risque lié à l'information, à maîtriser l'exposition juridique et à limiter le stockage de données redondantes ou obsolètes. Elle contribue à assurer la conformité à l'ISO/IEC 27001 et à des référentiels relatifs à la protection des données personnelles tels que le RGPD, en réduisant la conservation non autorisée d'informations à caractère personnel ou sensibles.

1.3 Un cadre structuré de conservation et d'élimination réduit les coûts d'exploitation, améliore les performances des systèmes et renforce la préparation aux audits. Pour les PME disposant de capacités informatiques limitées, il fournit un moyen pratique de gérer de manière responsable les actifs informationnels numériques et physiques.

2. Champ d'application

2.1 Cette politique s'applique à :

2.1.1 Tous les enregistrements, fichiers, journaux, communications et ensembles de données créés, collectés, traités ou stockés par l'organisation

2.1.2 Tous les employés, prestataires et fournisseurs externes manipulant des données de l'organisation

2.1.3 Tous les formats de données (par exemple : papier, électronique, image, audio ou journal) et tous les supports de stockage (par exemple : disques locaux, services cloud, serveurs de messagerie, sauvegardes)

2.2 Le champ d'application couvre :

2.2.1 Les documents métier (par exemple : factures, contrats, rapports de projet)

2.2.2 Les enregistrements opérationnels (par exemple : journaux, historiques d'accès, instantanés de sauvegarde)

2.2.3 Les données à caractère personnel (par exemple : dossiers RH, communications clients, enregistrements de support)

2.2.4 Les données hébergées en interne, en externe ou dans des systèmes hybrides

2.2.5 Les données archivées et les sauvegardes, qu'elles soient actives ou au repos

2.3 Toutes les étapes du cycle de vie des données entrent dans le champ d'application, de leur création à leur élimination autorisée.

3. Objectifs

3.1 Définir des règles de conservation cohérentes sur la base de critères juridiques, opérationnels et réglementaires.

3.2 Prévenir la suppression prématurée d'enregistrements critiques et éliminer l'accumulation inutile de données.

3.3 Garantir une élimination des données sécurisée, irréversible et appropriée lorsque leur conservation n'est plus requise.

3.4 Attribuer la responsabilité de l'application des décisions de conservation et de suppression dans un contexte de ressources limitées propre aux PME.

3.5 Fournir une documentation compatible avec les exigences d'audit afin de démontrer la diligence raisonnable au regard de l'ISO/IEC 27001, du RGPD, de NIS2 et d'autres référentiels.

3.6 Promouvoir un traitement sécurisé des données tout au long de leur cycle de vie sans imposer de charge technique excessive au personnel non spécialiste.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve la présente politique et en assume la responsabilité.

4.1.2 Veille à ce que les procédures de conservation et d'élimination soient mises en œuvre d'une manière cohérente avec les risques juridiques et métier.

4.1.3 Autorise les dérogations et les gels juridiques lorsque nécessaire.

4.1.4 Déclenche les revues de la politique et approuve les mises à jour en fonction des évolutions métier ou réglementaires.

4.2 Propriétaire de données désigné

4.2.1 Est désigné pour chaque catégorie de données (par exemple : finance, RH, dossiers clients).

4.2.2 Classe les enregistrements et détermine la durée de conservation appropriée sur la base de la politique et des exigences juridiques.

4.2.3 Autorise la suppression lorsque les exigences de conservation sont satisfaites.

4.2.4 Appuie les audits internes en fournissant le contexte relatif à la logique de conservation et aux opérations d'élimination.

[... 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 lors de :

9.1.1 Changements dans les lois applicables (par exemple : protection des données, reporting financier)

9.1.2 Adoption de nouveaux systèmes ou processus affectant le cycle de vie des données

9.1.3 Constats d'audit ou incidents révélant des lacunes dans les pratiques de conservation

9.2 Les revues doivent garantir que le registre de conservation demeure complet et reflète toutes les principales catégories d'enregistrements.

9.3 Les mises à jour de la politique doivent être approuvées par le DG et communiquées au personnel concerné. La version la plus récente doit être accessible et soumise au contrôle de version.

10. Politiques associées et articulations

10.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : définit la responsabilité de la politique et l'autorité en matière d'exceptions.

10.2 P13S – Politique de classification et d'étiquetage des données : détermine la manière dont les règles de conservation s'alignent sur la classification des données.

10.3 P12S – Politique de gestion des actifs : régit les supports de stockage contenant des données soumises à conservation/élimination.

10.4 P17S – Politique de protection des données et de la vie privée : garantit la minimisation des données et soutient le traitement licite de l'information au titre du RGPD.

10.5 P30S – Politique de réponse aux incidents : s'applique lorsque des défaillances de conservation ou d'élimination entraînent une exposition potentielle des données.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 6.1.3 : exige le traitement des risques liés à l'information, y compris les risques liés à la conservation.

11.1.2 Article 8.1 : définit les contrôles opérationnels du cycle de vie.

11.2 ISO/IEC 27002

11.2.1 Mesure 5.33 : fournit des lignes directrices pour définir les durées de conservation et les méthodes de destruction sécurisée.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11 : impose la conservation des journaux d'audit.

11.3.2 MP-6 : définit les procédures d'assainissement des supports.

11.3.3 SI-12 : traite des limites de conservation des données et de leur mise en application.

11.4 RGPD

11.4.1 Article 5(1)(e) : les données ne doivent pas être conservées plus longtemps que nécessaire.

11.4.2 Article 17 : le droit à l'effacement s'applique lorsque les données ne sont plus conservées sur une base légale.

11.5 NIS2

11.5.1 Article 21(2)(a) : exige des politiques organisationnelles adaptées au risque, y compris pour la gestion du cycle de vie.

11.6 DORA

11.6.1 Article 5(1) : la gestion des risques liés aux TIC inclut la disponibilité et la suppression des données.

11.7 COBIT 2019

11.7.1 BAI03.04 : impose des contrôles du cycle de vie de l'information.

11.7.2 DSS01.06 : prévoit des procédures d’élimination sécurisée dans le cadre de la protection des actifs informationnels.