					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P14					Titre du document : **Politique de conservation des données et d'élimination sécurisée**							
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, 8.1	
ISO/IEC 27002:2022	Mesures 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
RGPD de l'UE	Articles 5(1)(e), 17, 32	
NIS2 de l'UE	Article 21(2)(a-e)	
DORA de l'UE	Articles 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Objet

1.1 La présente politique a pour objet de définir les exigences organisationnelles relatives à la conservation des données et à leur élimination sécurisée sur l'ensemble du cycle de vie de l'information. Elle garantit la conformité aux obligations légales, réglementaires et contractuelles applicables et prévient l'accumulation inutile ou risquée de données.

1.2 La présente politique soutient la mise en œuvre de l'ISO/IEC 27001:2022 en imposant la maîtrise des durées de conservation des données et des pratiques d'élimination irréversible. Elle permet une documentation traçable des enregistrements, impose une conservation alignée sur le niveau de classification et garantit la préparation aux audits, aux inspections réglementaires et aux procédures de communication de pièces dans le cadre d'un contentieux.

1.3 Elle vise en outre à préserver la confidentialité, l'intégrité et la disponibilité des données, tout en réduisant le risque métier, les inefficacités opérationnelles et l'exposition aux atteintes à la vie privée résultant d'une conservation ou d'une destruction inappropriée des données.

2. Champ d'application

2.1 La présente politique s'applique à tous les actifs informationnels physiques et numériques détenus, traités ou conservés par l'organisation, y compris ceux placés sous le contrôle de tiers, de filiales ou de prestataires d'externalisation.

2.2 Le champ d'application inclut notamment, sans s'y limiter :

2.2.1 les documents, fichiers et enregistrements, sous format numérique ou papier ;

2.2.2 les bases de données et les archives ;

2.2.3 les courriels et les journaux de messagerie instantanée ;

2.2.4 les sauvegardes, les journaux système et les pistes d'audit ;

2.2.5 le code source, les données applicatives et les actifs hébergés dans le cloud ;

2.2.6 les supports amovibles et les équipements obsolètes contenant des données.

2.3 La politique encadre à la fois les enregistrements opérationnels et les jeux de données réglementés (par exemple les contenus financiers, juridiques, RH, liés aux clients et pertinents pour l'audit), quel que soit leur emplacement de stockage ou le système concerné.

2.4 Elle s'applique à l'ensemble des départements de l'organisation ainsi qu'aux employés, prestataires et fournisseurs impliqués dans la création, le stockage, la gestion ou l'élimination des données.

3. Objectifs

3.1 Garantir que les données ne sont conservées que pendant la durée nécessaire au regard des exigences légales, contractuelles ou opérationnelles, puis qu'elles sont éliminées de manière sécurisée lorsqu'elles ne sont plus requises.

3.2 Prévenir la suppression prématurée, non autorisée ou accidentelle des enregistrements nécessaires aux opérations en cours, à la conformité, aux contentieux ou aux besoins d'audit.

3.3 Définir et appliquer des calendriers de conservation cohérents fondés sur la classification de l'information, le type d'actif, les exigences légales applicables et l'exposition au risque.

3.4 Protéger la vie privée et la confidentialité des données pendant leur période de conservation et au moment de leur élimination, y compris par le respect des droits des personnes concernées (par exemple l'effacement au titre de l'article 17 du RGPD).

3.5 Garantir que toutes les méthodes d'élimination des données sont irréversibles, dûment documentées et conformes à des normes reconnues telles que le NIST SP 800-88.

3.6 Réduire les inefficacités opérationnelles, les surcoûts et l'exposition juridique causés par une conservation excessive ou par des données historiques non maîtrisées.

3.7 Soutenir les objectifs de continuité d'activité et de reprise après sinistre au moyen d'une gouvernance intégrée de la conservation des sauvegardes et de pratiques d'archivage des données juridiquement opposables.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve la présente politique et veille à la mise à disposition d'un financement, de ressources et d'une intégration appropriés dans les programmes de gestion des risques et de conformité de l'organisation.

4.1.2 Assume la responsabilité globale de la conformité légale et réglementaire relative à la conservation des données et à leur élimination sécurisée.

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

4.2.1 Est propriétaire de la présente politique et responsable de la définition et de la revue de la gouvernance de la conservation et de l'élimination en cohérence avec le SMSI.

4.2.2 Veille à ce que les exigences de conservation et d'élimination fondées sur la classification soient mises en œuvre dans les unités métier et les systèmes techniques.

4.2.3 Surveille la conformité à la politique et impose des actions correctives lorsque nécessaire.

[... 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 annuelle ou lorsqu'une des conditions suivantes est remplie :

9.1.1 des modifications des lois ou réglementations applicables affectant la conservation des données (par exemple mises à jour du RGPD, des codes fiscaux ou de DORA) ;

9.1.2 des révisions du cadre de classification ou des processus métier ayant une incidence sur les étapes du cycle de vie des données ;

9.1.3 l'introduction de nouveaux systèmes informatiques, de nouvelles plateformes d'archivage ou de nouvelles technologies d'élimination des supports ;

9.1.4 des constats d'audit interne ou des recommandations réglementaires mettant en évidence des lacunes dans les pratiques de conservation ou d'élimination.

9.2 La revue doit être pilotée par le RSSI et le Délégué à la protection des données (DPO), avec la contribution de la direction juridique, de la conformité, de l'informatique et des unités métier.

9.3 Le calendrier maître de conservation des données (MDRS) et le registre d'élimination doivent être revus en parallèle afin de garantir que :

9.3.1 les calendriers restent exacts et reflètent les besoins opérationnels, juridiques et réglementaires ;

9.3.2 la documentation d'élimination est complète et compatible avec les exigences d'audit ;

9.3.3 les enregistrements de gel légal sont validés et levés lorsque cela est approprié.

9.4 Toute mise à jour de la politique doit :

9.4.1 être formellement versionnée et conservée dans le référentiel documentaire du SMSI ;

9.4.2 inclure un historique des versions et une justification des changements ;

9.4.3 être approuvée par la haute direction ;

9.4.4 être communiquée au personnel concerné avec des supports de formation ou d'orientation mis à jour.

9.5 En cas de changement significatif de la politique, les employés concernés doivent suivre une formation ciblée dans les 30 jours suivant sa publication afin de garantir le maintien de la conformité.

9.6 Politiques associées et articulations

10. Politiques associées et articulations

10.1.1 P4 - Politique de contrôle d'accès : garantit que seules les personnes autorisées accèdent aux données pendant leur durée de conservation et que les données arrivées à échéance font l'objet de restrictions dans l'attente de leur élimination.

10.1.2 P12 - Politique de gestion des actifs : identifie les actifs contenant des données nécessitant une élimination planifiée et suit leur cycle de vie depuis l'acquisition jusqu'à la destruction.

10.1.3 P13 - Politique de classification et d'étiquetage des données : guide les décisions de classification qui influencent directement la durée de conservation des données et la méthode d'élimination requise.

10.1.4 P15 - Politique de sauvegarde et de restauration : définit les durées de conservation et les procédures d'élimination des supports de sauvegarde et des actifs de données répliquées.

10.1.5 P18 - Politique des contrôles cryptographiques : prend en charge l'effacement cryptographique à des fins d'élimination et impose le chiffrement pendant le stockage des données jusqu'à leur destruction.

10.1.6 P30 - Politique de réponse aux incidents : est activée lorsque l'élimination inappropriée entraîne une perte potentielle de données, une violation ou un manquement réglementaire.

10.2 Chaque politique associée contribue à l'application d'un modèle cohérent de gouvernance des données couvrant la classification, la maîtrise du cycle de vie, l'accès et la préparation aux audits.

11. Normes et référentiels de référence

11.1 La présente politique s'aligne sur des normes et référentiels réglementaires mondialement reconnus qui définissent des pratiques de cycle de vie des données sûres, conformes et efficaces.

11.2 ISO/IEC 27001 :

11.2.1 Article 6.1.3 - plan de traitement des risques : soutient l'atténuation des risques associés à la conservation excessive, aux violations de données ou aux défaillances d'élimination.

11.2.2 Article 8.1 - planification et maîtrise opérationnelles : établit les contrôles du cycle de vie qui encadrent le stockage, l'archivage et la destruction.

11.3 ISO/IEC 27002:2022 - Mesures 5.10, 5.12, 5.30, 5 : fournissent des orientations pratiques sur l'utilisation acceptable des données, la justification de la conservation, la suppression contrôlée et la tenue d'enregistrements juridiquement opposable alignée sur l'appétence au risque de l'organisation.

11.4 NIST SP 800-53 Rev. 5 :

11.4.1 AU-11 - conservation des enregistrements d'audit : garantit un stockage suffisant des journaux d'audit et des éléments de preuve de conformité.

11.4.2 MP-6 - assainissement des supports : impose des méthodes de destruction sécurisées et documentées pour les supports physiques et électroniques.

11.4.3 SI-12 - traitement de l'information : impose un traitement approprié des données aligné sur les contrôles de conservation et d'élimination.

11.4.4 PL-2 - plan de sécurité et de protection de la vie privée du système : impose une documentation propre au système sur la gestion du cycle de vie des données et les dispositions d'élimination sécurisée.

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

11.5.1 Article 5(1)(e) - minimisation des données et limitation de la conservation : exige que les données ne soient pas conservées plus longtemps que nécessaire.

11.5.2 Article 17 - droit à l'effacement (« droit à l'oubli ») : exige la suppression rapide et définitive des données à caractère personnel sur demande valide.

11.5.3 Article 32 - sécurité du traitement : renforce la protection des données pendant leur conservation et impose la destruction sécurisée des enregistrements arrivés à échéance.

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

11.6.1 Article 21(2)(a-e) : impose aux entités d'adopter des politiques et des mesures techniques de traitement sécurisé des données, y compris des limitations de stockage et des méthodes d'élimination.

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

11.7.1 Article 5 - gouvernance et contrôle : impose une gestion structurée des risques liés aux TIC, y compris la gestion sécurisée du cycle de vie de l'information.

11.7.2 Article 9 - cadre de gestion des risques liés aux TIC : impose des politiques relatives à la conservation, à la destruction et à la conformité légale et réglementaire des opérations numériques.

11.8 COBIT 2019 :

11.8.1 DSS01 - gestion des opérations : soutient le suivi de la conservation et la cohérence entre les systèmes de données.

11.8.2 DSS05 - gestion des services de sécurité : garantit la protection des données stockées et archivées jusqu'à leur élimination sécurisée.

11.8.3 MEA03 - surveiller, évaluer et apprécier la conformité : permet l'audit de l'application des règles de conservation, des procédures de suppression et du respect des exigences réglementaires.