					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P18S					Titre du document : **Politique relative aux contrôles cryptographiques**							
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	Article 8	
ISO/IEC 27002:2022	Mesures 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 à SC-17	
NIS2 (UE)	Articles 21(2)(d), 21(2)(e)	
DORA (UE)	Articles 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
RGPD (UE)	Articles 32(1)(a), 34	

1. Objet

1.1 La présente politique définit les exigences obligatoires relatives à l'utilisation du chiffrement et des contrôles cryptographiques afin de protéger la confidentialité, l'intégrité et l'authenticité des données métier et des données à caractère personnel.

1.2 Elle impose l'utilisation appropriée d'outils cryptographiques dans les systèmes, les équipements et les services cloud au sein d'un environnement de petite entreprise.

1.3 La présente politique contribue directement à la certification ISO/IEC 27001:2022 et aide l'organisation à respecter les obligations légales du règlement général sur la protection des données (RGPD), de la directive NIS2 et du règlement sur la résilience opérationnelle numérique (DORA).

1.4 Les contrôles cryptographiques couverts comprennent le chiffrement des données, la gestion des certificats, la gestion sécurisée des clés et les sauvegardes chiffrées.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 tous les employés, prestataires et tiers qui traitent des données de l'entreprise ;

2.1.2 tous les systèmes métier, terminaux et plateformes cloud utilisés pour stocker, transmettre ou consulter des informations confidentielles ;

2.1.3 tous les enregistrements personnels, financiers, juridiques ou sensibles classifiés conformément à la politique de classification des données de l'organisation ;

2.1.4 tous les contrôles cryptographiques, y compris les méthodes de chiffrement, les clés, les mots de passe, les certificats et les modules de sécurité.

2.2 La politique couvre les données au repos, les données en transit et les données en cours d'utilisation. Elle encadre également le chiffrement utilisé pour les sauvegardes, la messagerie électronique, les transferts de données externes et les sites web publics.

3. Objectifs

3.1 Garantir que les données sensibles et réglementées sont protégées en permanence au moyen de mesures cryptographiques appropriées.

3.2 Définir les responsabilités relatives au choix des outils de chiffrement, à leur configuration et à la gestion des clés.

3.3 Prévenir tout accès non autorisé, toute altération ou toute fuite de données en imposant des contrôles sécurisés de transmission et de stockage.

3.4 Respecter les exigences légales et réglementaires imposant le chiffrement des données à caractère personnel et des données métier.

3.5 Maintenir la sécurité opérationnelle et la disponibilité au moyen d'une gestion efficace des certificats et des clés cryptographiques.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Approuve la présente politique et veille à la mise en œuvre des exigences cryptographiques.

4.1.2 Examine les dérogations, les notifications de violation et la conformité des fournisseurs aux exigences de chiffrement.

4.1.3 Vérifie que les services externalisés ou cloud respectent les normes de chiffrement.

4.2 Prestataire de support informatique / Administrateur informatique interne

4.2.1 Met en œuvre et maintient les solutions de chiffrement (par exemple, chiffrement intégral du disque, certificats SSL/TLS, réseaux privés virtuels (VPN)).

4.2.2 Gère le cycle de vie des clés cryptographiques et les outils de stockage sécurisé.

4.2.3 Configure et surveille le chiffrement afin de protéger les sauvegardes, les sites web et les équipements.

[... 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 au moins une fois par an par le Directeur général, en coordination avec le prestataire de support informatique et le Coordinateur à la protection des données.

9.2 Déclencheurs de revue intermédiaire

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

9.2.1.1 évolution des normes ou protocoles cryptographiques (par exemple, obsolescence d'un algorithme) ;

9.2.1.2 introduction de nouveaux systèmes ou services cloud ;

9.2.1.3 violation ou incident impliquant une clé ou un certificat compromis ;

9.2.1.4 mises à jour légales ou réglementaires ayant une incidence sur les exigences de chiffrement.

9.3 Gestion des versions et communication

9.3.1 Toute modification de la politique doit être documentée dans un journal de gestion des versions.

9.3.2 Le personnel doit être informé des mises à jour et les versions précédentes doivent être archivées.

9.3.3 La dernière version approuvée doit être conservée dans le référentiel central des politiques.

10. Politiques associées et articulations

10.1 La présente politique doit être appliquée conjointement avec les politiques PME suivantes :

10.1.1 P12S – Politique de gestion des actifs : impose l'application du chiffrement aux actifs classifiés pendant le stockage, le transfert et l'élimination.

10.1.2 P14S – Politique de conservation et d'élimination des données : définit les durées de conservation et impose le stockage chiffré des données jusqu'à leur suppression sécurisée.

10.1.3 P17S – Politique de protection des données et de la vie privée : aligne le chiffrement sur les principes de protection des données et les exigences réglementaires prévues à l'article 32 du RGPD.

10.1.4 P22S – Politique de journalisation et de surveillance : impose la journalisation de l'utilisation des clés, des échecs de chiffrement et des dates d'expiration des certificats à des fins d'audit.

10.1.5 P30S – Politique de réponse aux incidents : détaille les procédures d'escalade, de confinement et de notification lorsque le chiffrement échoue ou que des clés sont compromises.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 8.1 – Exige la mise en œuvre de contrôles opérationnels, y compris le chiffrement, afin de gérer les risques de sécurité.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.24 – Décrit les exigences relatives à l'application du chiffrement pour assurer la confidentialité et l'intégrité.

11.2.2 Mesure 8.25 – Définit les exigences relatives à la gestion sécurisée des clés cryptographiques et des certificats.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Établit les exigences relatives à l'établissement et à la validation des clés cryptographiques.

11.3.2 SC-13 – Définit les exigences applicables à la génération des clés cryptographiques.

11.3.3 SC-17 – Couvre l'infrastructure à clé publique (PKI) et la gestion du cycle de vie des certificats.

11.3.4 SC-28 – Exige le chiffrement des données au repos.

11.3.5 SC-12 à SC-17 (famille) – Garantit que les protections cryptographiques sont correctement mises en œuvre dans l'ensemble des systèmes.

11.4 RGPD (UE)

11.4.1 Article 32(1)(a) – Exige des organisations qu'elles mettent en œuvre des mesures techniques telles que le chiffrement afin d'assurer la confidentialité des données.

11.4.2 Article 34 – Précise que le chiffrement peut dispenser les organisations de notifier une violation si les données étaient inintelligibles pour des personnes non autorisées.

11.5 Directive NIS2

11.5.1 Article 21(2)(d) – Exige un chiffrement efficace pour sécuriser les systèmes et les communications.

11.5.2 Article 21(2)(e) – Met l'accent sur la protection des données et l'atténuation des cybermenaces au moyen du chiffrement.

11.6 DORA (UE)

11.6.1 Article 6(2)(d) – Exige que les systèmes TIC maintiennent des canaux de communication sécurisés et le chiffrement.

11.6.2 Article 9(2)(f) – Implique, pour les entités financières, l'utilisation d'un chiffrement fort afin de protéger les communications numériques et les échanges de données.

11.7 COBIT 2019

11.7.1 DSS05.01 – Implique la protection des informations sensibles au moyen du chiffrement et de protocoles cryptographiques.

11.7.2 APO13.02 – Exige la mise en œuvre effective de contrôles de sécurité, y compris de mesures de protection cryptographiques, dans le cadre de la planification de la sécurité de l’information.