					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P18					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	Clause 8	-
ISO/IEC 27002:2022	Mesures 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 à SC-17, SC-28, SC-28(1), SC-12(3)	-
RGPD de l'UE	Article 32, Articles 33–34, Considérant 83	-
NIS2 de l'UE	Article 21(2)(d)	-
DORA de l'UE	Articles 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Objet

1.1 La présente politique définit les exigences obligatoires relatives à l'utilisation sécurisée et conforme des contrôles cryptographiques dans l'ensemble de l'organisation afin de garantir la confidentialité, l'intégrité et l'authenticité des informations sensibles et réglementées.

1.2 Le recours à la cryptographie constitue un fondement de la confiance dans les opérations de sécurité des données, soutient les communications sécurisées, permet le contrôle d'accès et contribue à la conformité réglementaire au moyen de pratiques efficaces de chiffrement et de gestion des clés.

1.3 La présente politique est alignée sur l'ISO/IEC 27001:2022, clause 8.1 et annexe A, mesure 8.24, et soutient les obligations juridiques et opérationnelles prévues par l'article 32 du RGPD, l'article 6(2)(d) de DORA et l'article 21 de NIS2. Elle soutient également les objectifs de COBIT 2019 relatifs aux services de sécurité et à la protection des actifs informationnels.

2. Champ d'application

2.1 La présente politique s'applique à toutes les unités organisationnelles, fonctions métier, ainsi qu'à l'ensemble du personnel et aux prestataires tiers intervenant dans l'utilisation, l'administration ou la mise en œuvre d'outils et de mécanismes cryptographiques.

2.2 Les environnements couverts incluent les systèmes de production, de développement, de préproduction, de sauvegarde et de reprise après sinistre dans lesquels des données sensibles sont transmises, traitées ou stockées.

2.3 Le champ d'application couvre l'ensemble des composants cryptographiques et des cas d'usage, y compris, sans s'y limiter :

2.3.1 Chiffrement symétrique et asymétrique

2.3.2 Signatures numériques et certificats

2.3.3 Algorithmes de hachage cryptographique

2.3.4 Génération, distribution et destruction sécurisées des clés

2.3.5 Transport Layer Security (TLS), chiffrement intégral du disque (FDE) et chiffrement au niveau des interfaces de programmation applicative (API)

2.3.6 Composants sécurisés tels que les modules matériels de sécurité (HSM), les modules de plateforme sécurisée (TPM) et les systèmes de gestion des clés (KMS)

2.4 La présente politique encadre l'utilisation de la cryptographie pour :

2.4.1 Les données classifiées comme Confidentielles, Hautement confidentielles ou Réglementées

2.4.2 L’authentification et la vérification des identités numériques

2.4.3 Les communications sécurisées avec des parties externes

2.4.4 La garde des clés et les mécanismes de double contrôle

3. Objectifs

3.1 Veiller à ce que les technologies cryptographiques soient sélectionnées, approuvées, mises en œuvre et maintenues conformément au risque métier, aux normes internationales et aux exigences réglementaires.

3.2 Établir une structure de gouvernance normalisée pour la gestion des services cryptographiques, avec des responsabilités clairement définies en matière de mise en œuvre, de validation et de gestion des dérogations.

3.3 Prévenir l’utilisation non autorisée, la mauvaise configuration ou l’obsolescence des algorithmes et contrôles cryptographiques au moyen d’un processus formel d’approbation et de revue.

3.4 Veiller à ce que les contrôles cryptographiques soient intégrés dès la phase de conception des systèmes et validés régulièrement afin de prévenir l’exposition des données, la compromission des clés ou l’affaiblissement des protocoles.

3.5 Imposer la gestion du cycle de vie de l’ensemble des clés cryptographiques, y compris leur génération, stockage, utilisation, rotation, révocation et destruction sécurisée.

3.6 Se conformer aux réglementations internationales et régionales imposant le chiffrement et le traitement sécurisé des données, notamment le RGPD, DORA, NIS2 et COBIT 2019.

4. Rôles et responsabilités

4.1 Responsable de la sécurité de l’information / RSSI

4.1.1 Est responsable de la présente politique et veille à son alignement avec le système de management de la sécurité de l’information (SMSI) et l’ISO/IEC 27001, annexe A, mesure 8.24.

4.1.2 Approuve l’utilisation des algorithmes et des contrôles cryptographiques et veille au respect des exigences de conformité dans l’ensemble de l’organisation.

4.2 Responsable des opérations cryptographiques / Architecte sécurité

4.2.1 Assure l’exploitation quotidienne et l’administration des systèmes cryptographiques.

4.2.2 Tient à jour la liste des méthodes cryptographiques approuvées (ACML) et le registre de gestion des clés.

4.2.3 Réalise les revues de conception cryptographique (CDR) et évalue les nouvelles technologies cryptographiques.

[... 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 par le Responsable de la sécurité de l’information et le Responsable des opérations cryptographiques.

9.2 Les déclencheurs de revue incluent :

9.2.1 La découverte de vulnérabilités cryptographiques (par exemple affaiblissement d’algorithme, attaques quantiques)

9.2.2 Des évolutions réglementaires imposant la mise à jour des normes de chiffrement

9.2.3 Des constats opérationnels ou d’audit révélant des lacunes de la politique

9.2.4 Des mises à niveau d’outils cryptographiques ou des changements d’architecture

9.3 Les mises à jour doivent faire l’objet d’une gestion de version dans le registre de contrôle documentaire du SMSI et être communiquées à :

9.3.1 Tous les administrateurs disposant de rôles d'accès cryptographiques

9.3.2 Les équipes de développement et les responsables DevSecOps

9.3.3 Les tiers soumis à des obligations contractuelles en matière de chiffrement

9.4 L'équipe SMSI doit veiller à ce que les versions remplacées soient archivées et ne soient plus référencées dans les procédures opérationnelles.

10. Politiques associées et articulations

10.1 P1 - Politique de sécurité de l'information. Fournit le cadre de gouvernance de base pour l'ensemble des mesures de sécurité, y compris l'application des contrôles cryptographiques, la protection des actifs et les communications sécurisées.

10.2 P4 - Politique de contrôle d'accès. Garantit que l'accès logique aux composants cryptographiques et aux systèmes de gestion du chiffrement est strictement limité sur la base du moindre privilège et de la séparation des tâches.

10.3 P6 - Politique de gestion des risques. Soutient l'évaluation des risques liés aux contrôles cryptographiques et documente la stratégie de traitement des risques pour les dérogations, l'obsolescence des algorithmes ou les scénarios de compromission de clés.

10.4 P12 - Politique de gestion des actifs. Implique la classification des données sensibles et des actifs matériels, ce qui détermine directement les exigences cryptographiques et les obligations de garde des clés.

10.5 P13 - Politique de classification et d'étiquetage des données. Définit les niveaux de classification (par exemple Confidentiel, Réglementé) qui déclenchent des exigences spécifiques de chiffrement en transit et au repos.

10.6 P14 - Politique de conservation et d'élimination des données. Précise les procédures d'élimination sécurisée des supports de stockage chiffrés et des composants cryptographiques en fin de vie.

10.7 P30 - Politique de réponse aux incidents. Décrit la stratégie de l'organisation en réponse à une compromission de clé, à un usage abusif de certificat ou à des vulnérabilités algorithmiques suspectées, y compris la révocation rapide et le signalement des violations.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 - Planification et maîtrise opérationnelles : impose des contrôles de sécurité techniques, y compris des mesures cryptographiques, dans le cadre des dispositifs de protection opérationnels.

11.2 ISO/IEC 27002:2022

11.2.1 Mesures 8.24, 8.25, 8 : fournissent des orientations de mise en œuvre sur les objectifs des contrôles cryptographiques, la sélection des algorithmes, l'application des protocoles et la gestion du cycle de vie des certificats.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Établissement des clés cryptographiques : garantit la génération et l'échange sécurisés des clés de chiffrement. P18 définit la manière dont les clés symétriques et asymétriques doivent être générées et échangées au moyen d'algorithmes et de protocoles approuvés.

11.3.2 SC-13 - Protection cryptographique : impose l'usage de la cryptographie pour protéger la confidentialité et l'intégrité des informations. P18 impose le chiffrement des données au repos et en transit selon leur classification, avec des normes algorithmiques alignées sur NIST FIPS 140-3.

11.3.3 SC-17 - Certificats d'infrastructure à clé publique (PKI) : exige la mise en œuvre d'une PKI pour prendre en charge l'authentification et les signatures numériques. P18 décrit l'usage de la PKI pour sécuriser les communications, les identités système et les accès administratifs.

11.3.4 SC-28, SC-28(1) - Protection des informations au repos et en transit : impose le chiffrement des données lorsqu'elles sont stockées ou transmises sur des réseaux non fiables. P18 précise l'application de TLS, des tunnels VPN, du chiffrement intégral du disque et des méthodes de stockage sécurisées pour les données sensibles.

11.3.5 SC-12(3) - Génération de clés symétriques pour un stockage et une distribution sécurisés : porte sur la génération et le traitement sécurisés des clés symétriques. P18 impose l'usage de générateurs de nombres aléatoires robustes, de politiques de rotation des clés et de coffres-forts de clés sécurisés pour les opérations cryptographiques.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 32 - Sécurité du traitement : recommande explicitement le chiffrement comme mesure de réduction des risques pour les données à caractère personnel.

11.4.2 Considérant 83 : souligne le chiffrement comme contrôle destiné à empêcher les accès non autorisés aux données.

11.4.3 Articles 33 et 34 : le chiffrement peut dispenser les organisations de certaines obligations de notification de violation lorsqu'il est effectif.

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

11.5.1 Article 21(2)(d) : exige des mesures techniques et organisationnelles, y compris des protections cryptographiques, afin de maintenir la disponibilité et l'intégrité des services.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 6(2)(d) : les établissements financiers doivent sécuriser les données, notamment au moyen d'un chiffrement robuste des informations critiques.

11.6.2 Article 11(1)(c) : impose des contrôles de traitement sécurisé des données pour les prestataires tiers de services TIC.

11.7 COBIT 2019

11.7.1 DSS05.01 - Protéger les actifs informationnels : exige l'utilisation du chiffrement et de la gestion des clés pour protéger les données contre les accès non autorisés.

11.7.2 DSS06.06 - Tests de sécurité gérés : recommande la validation de la conformité cryptographique dans le cadre des évaluations de vulnérabilité.

11.7.3 MEA03 - Surveiller, évaluer et apprécier la conformité : impose une assurance continue de l'efficacité des contrôles cryptographiques.