Politique Cryptographie ISO 27001 : Modèle Word [A.8.24 + ANSSI]

15 mai 2026 • Mis à jour le 17 mai 2026 • 24 min de lecture • 2518 mots •

27 vues •

Télécharger le PDF

> Le contrôle A.8.24 ISO 27001:2022 impose une politique cryptographique formalisée. Ce modèle Word liste les algorithmes autorisés par l'ANSSI (AES-256-G.

À RETENIR

🔐 Template gratuit · Word

Le contrôle A.8.24 ISO 27001:2022 impose une politique cryptographique formalisée. Ce modèle Word liste les algorithmes autorisés par l'ANSSI (AES-256-GCM, ChaCha20, RSA-3072, ECDSA P-256), la gestion des clés (HSM/KMS) et la rotation.

📥 Télécharger (Word gratuit)

La **politique de cryptographie** est le document de référence qui définit l'utilisation des techniques cryptographiques au sein du Système de Management de la Sécurité de l'Information (SMSI). Le contrôle **A.8.24** d'ISO/IEC 27001:2022 impose d'établir et de mettre en œuvre une politique formalisée sur l'utilisation de la cryptographie pour protéger la confidentialité, l'authenticité et l'intégrité des informations. Cette politique doit couvrir les algorithmes autorisés et prohibés, les longueurs de clés minimales, les protocoles cryptographiques approuvés, et la gestion du cycle de vie des clés cryptographiques (génération, distribution, stockage, rotation, révocation, destruction). Ce modèle Word, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO 27001, s'aligne sur les recommandations de l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) publiées dans ses guides de référence (RGS — Référentiel Général de Sécurité, et guide "Cryptographie" de 2021). Les algorithmes recommandés incluent AES-256-GCM pour le chiffrement symétrique, ChaCha20-Poly1305 comme alternative, RSA-3072 et ECDSA P-256 pour la cryptographie asymétrique, SHA-256 et SHA-3 pour le hachage, et TLS 1.3 pour les communications. La politique cryptographique s'articule étroitement avec la politique de gestion des accès logiques, la politique de classification de l'information (le niveau de chiffrement requis dépend de la classification), et les contrôles de sécurité réseau (A.8.20-23). À l'ère de l'informatique quantique en développement, une politique cryptographique à jour doit