



Politique DLP (Data Leakage Prevention) ISO 27001 : Word [A.8.12]

15 mai 2026 • Mis à jour le 17 mai 2026 • 44 min de lecture • 4391 mots • 21 vues •

Le contrôle A.8.12 ISO 27001:2022 impose la prévention des fuites d'information. Ce modèle Word couvre les solutions DLP (endpoint, réseau, cloud), les.



À RETENIR

Template gratuit · Word — Politiques

Le contrôle A.8.12 ISO 27001:2022 impose la prévention des fuites d'information. Ce modèle Word couvre les solutions DLP (endpoint, réseau, cloud), les règles de détection par type de donnée et les workflows de remédiation.

 **Télécharger (Word gratuit)**

La prévention des fuites de données (Data Leakage Prevention, DLP) constitue l'un des piliers fondamentaux de la sécurité de l'information dans le cadre ISO 27001:2022. Le contrôle A.8.12 impose aux organisations de mettre en place des mesures techniques et organisationnelles permettant de détecter et de prévenir la divulgation non autorisée d'informations sensibles, qu'elles soient en transit, en cours d'utilisation ou au repos. Une politique DLP efficace combine la classification des données, la surveillance des flux d'information, les contrôles techniques sur les terminaux et les canaux réseau, ainsi que des procédures de réponse aux incidents de fuite. Pour les organisations certifiées ISO 27001 ou en cours de certification, la politique DLP doit s'intégrer dans le système de management de la sécurité de l'information (SMSI) et être alignée avec les exigences RGPD en matière de protection des données personnelles, les obligations NIS 2 pour les opérateurs d'importance vitale, et les recommandations ANSSI en matière de protection du patrimoine informationnel. Ce guide complet vous accompagne dans la rédaction, le déploiement et l'audit de votre politique DLP conformément aux exigences ISO 27001:2022.

Contexte réglementaire et normatif du contrôle A.8.12

Le contrôle A.8.12 de la norme ISO 27001:2022 s'inscrit dans le thème 8 « Contrôles technologiques » et traite spécifiquement de la
