Politique Anti-Malware & EDR ISO 27001 : Word [A.8.7]

15 mai 2026 • Mis à jour le 17 mai 2026 • 29 min de lecture • 2597 mots • 20 vues •

> Le contrôle A.8.7 ISO 27001:2022 (protection contre les logiciels malveillants) couvre antivirus, EDR/XDR et durcissement applicatif. Ce modèle Word lis.

À RETENIR

Template gratuit · Word — Politiques

Le contrôle A.8.7 ISO 27001:2022 (protection contre les logiciels malveillants) couvre antivirus, EDR/XDR et durcissement applicatif. Ce modèle Word liste les exigences techniques minimales et les processus de surveillance, alerting et remédiation.

Télécharger (Word gratuit)

La **politique anti-malware et EDR ISO 27001** formalise les exigences de protection contre les logiciels malveillants dans le cadre du contrôle **A.8.7 — Protection contre les maliciels** de l'Annexe A ISO/IEC 27001:2022. Les ransomwares, chevaux de Troie, malwares sans fichier (fileless), logiciels espions et autres codes malveillants représentent la première cause de compromission des systèmes d'information en France selon le panorama annuel de la cybermenace ANSSI. Sans politique anti-malware structurée, documentée et opérationnelle, aucune organisation n'est en mesure de démontrer la maîtrise de ce risque fondamental lors d'un audit de certification ISO 27001. La norme exige que des mesures de détection, de prévention et de récupération soient mises en œuvre pour protéger contre les maliciels, que les utilisateurs soient sensibilisés, et que la mise à jour des définitions et logiciels de détection soit assurée. Ce template Word, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO 27001, couvre l'architecture de protection anti-malware à plusieurs couches (endpoint, réseau, messagerie, web, cloud), les exigences minimales pour les solutions antivirus traditionnelles et EDR/XDR modernes, les règles de déploiement obligatoire sur tous les équipements du périmètre, les procédures d'alerting et de remédiation, les exceptions justifiées (systèmes legacy incompatibles), et les indicateurs de performance (taux de couverture, délai de mise à jour des signatures). Il s'adresse aux RSSI qui définissent la stratégie de protection des endpoints, aux équipes IT qui déploient et opèrent les solutions anti-malware, aux auditeurs internes qui vérifient la conformité technique des déploiements, et aux responsables achat qui sélectionnent les outils de protection. À lire en parallèle avec la politique de logging et monitoring (A.8.15-16) pour