Politique Sécurité Réseau ISO 27001 : Word [A.8.20-22]

15 mai 2026 • Mis à jour le 17 mai 2026 • 37 min de lecture • 3443 mots • 18 vues •

Les contrôles A.8.20 à A.8.22 couvrent les contrôles réseau, segmentation et services de communication. Ce modèle Word documente la segmentation Tier 0/.

À RETENIR

Template gratuit · Word — Politiques

Les contrôles A.8.20 à A.8.22 couvrent les contrôles réseau, segmentation et services de communication. Ce modèle Word documente la segmentation Tier 0/1/2, le déploiement Zero Trust, les VPN/SASE et la gestion des règles firewall.

Télécharger (Word gratuit)

La **politique de sécurité réseau** ISO 27001 est l'un des documents techniques les plus attendus par les auditeurs de certification. Elle répond aux exigences des contrôles **A.8.20 — Sécurité des réseaux**, **A.8.21 — Sécurité des services réseau** et **A.8.22 — Filtrage du Web** de l'Annexe A ISO/IEC 27001:2022. Ces trois contrôles du thème Technologique couvrent l'intégralité de la protection du périmètre réseau : segmentation des zones de confiance, contrôle des flux entrants et sortants, gestion sécurisée des services réseau (DNS, DHCP, NTP, SNMP), surveillance des communications, et filtrage des accès Internet. Dans le contexte actuel où les attaques par mouvement latéral, ransomware et exfiltration de données via le réseau constituent la majorité des compromissions réussies, une politique réseau rigoureuse n'est pas un simple exercice de conformité — c'est une nécessité opérationnelle. Ce modèle Word, développé par **Ayi NEDJIMI**, consultant cybersécurité et Lead Implementer ISO 27001, couvre la segmentation réseau selon le modèle Tier 0/1/2 (Active Directory), l'architecture Zero Trust et micro-segmentation, les règles de gestion des accès distants (VPN, ZTNA, SASE), la politique de gestion des règles firewall (changement, révision, décommissionnement), la surveillance réseau et la détection d'anomalies (NDR), et les exigences de sécurité pour les services réseau tiers et cloud. Il s'adresse aux RSSI qui formalisent l'architecture de sécurité réseau, aux équipes Infrastructure/Network qui implémentent les contrôles, aux administrateurs système qui gèrent les règles firewall au quotidien, et aux auditeurs internes qui vérifient la conformité des configurations réseau. La politique réseau doit être lue en parallèle avec la politique de logging et monitoring (A.8.15-16) et la politique de sécurité physique (A.7) pour couvrir l'ensemble du périmètre de sécurité infrastructure.