Politique Services Cloud ISO 27001 : Word [A.5.23]

15 mai 2026 • Mis à jour le 17 mai 2026 • 30 min de lecture • 2804 mots •

17 vues •

Le contrôle A.5.23 ISO 27001:2022 régit l'utilisation et le ciblage des services cloud (SaaS, IaaS, PaaS). Ce modèle Word définit le processus de qualif.

À RETENIR

Template gratuit · Word — Politiques

Le contrôle A.5.23 ISO 27001 2022 régit l'utilisation et le ciblage des services cloud (SaaS, IaaS, PaaS). Ce modèle Word définit le processus de qualification, les clauses DPA et les contrôles continus à imposer aux prestataires cloud.

Télécharger (Word gratuit)

La **politique des services cloud ISO 27001** formalise les exigences de sécurité applicables aux services cloud (SaaS, IaaS, PaaS, FaaS) dans le cadre du contrôle **A.5.23 — Sécurité de l'information pour l'utilisation des services en nuage** de l'Annexe A ISO/IEC 27001:2022. Ce contrôle, nouveau dans la version 2022, reconnaît explicitement le rôle prépondérant du cloud dans les infrastructures modernes et impose que les exigences de sécurité de l'information relatives à l'acquisition, à l'utilisation, à la gestion et à la sortie des services cloud soient définies selon l'approche de l'organisation en matière de gestion des risques. Le cloud a fondamentalement transformé le modèle de responsabilité en sécurité : dans un modèle de responsabilité partagée, le fournisseur cloud sécurise l'infrastructure sous-jacente, mais la sécurisation des données, des accès, des configurations et des applications reste la responsabilité du client. Des failles de configuration cloud — buckets S3 publics, permissions IAM trop larges, journalisation désactivée — sont à l'origine de la majorité des incidents de fuite de données liés au cloud. Ce template Word, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO 27001, couvre le processus de qualification des prestataires cloud (critères de sélection, certifications attendues comme SecNumCloud, ISO 27017, ISO 27018, SOC 2 Type II), les clauses contractuelles de sécurité à inclure dans les accords cloud (DPA RGPD, droits d'audit, notifications d'incidents, engagement de confidentialité, portabilité des données), les contrôles de sécurité à configurer dans chaque environnement cloud (IAM, logging, chiffrement, configuration baseline), et le processus de sortie sécurisée d'un prestataire cloud (migration des données, révocation des accès, destruction certifiée des données). Il s'adresse aux RSSI qui définissent la stratégie cloud sécurisée de l'organisation, aux équipes DevOps et