



Politique Mots de Passe ISO 27001 : Modèle Word [NIST + ANSSI]



15 mai 2026



Mis à jour le 17 mai 2026



21 min de lecture



2440 mots



15 vues



Télécharger le PDF

Conforme aux dernières recommandations NIST SP 800-63B et ANSSI 2015, longueur minimum 14 caractères, rotation conditionnelle (pas systématique), MFA o.

À RETENIR

Template gratuit · Word

Conforme aux dernières recommandations NIST SP 800-63B et ANSSI 2026 (longueur minimum 14 caractères, rotation conditionnelle (pas systématique), MFA obligatoire pour les admins, blocage des dictionnaires connus).

 **Télécharger (Word gratuit)**

La **politique de mots de passe** est l'un des documents de sécurité les plus connus mais aussi les plus mal rédigés des organisations. Pendant des années, la doctrine dominante imposait des mots de passe complexes (majuscules, chiffres, caractères spéciaux) avec rotation obligatoire tous les 90 jours — une approche que les recommandations actuelles du **NIST (SP 800-63B)** et de l'**ANSSI** ont profondément remise en question. Les recherches montrent que cette approche "complexité + rotation forcée" conduit les utilisateurs à choisir des mots de passe faibles mais mémorables (P@ssw0rd1, P@ssw0rd2...) ou à les noter physiquement, ce qui réduit paradoxalement la sécurité. Le contrôle **A.5.1** d'ISO/IEC 27001:2022 (Authentication information) et le contrôle **A.8.5** (Secure authentication) encadrent les exigences d'authentification. La doctrine moderne repose sur trois piliers : longueur plutôt que complexité (14 caractères minimum, phrases de passe recommandées), rotation conditionnelle uniquement en cas de suspicion de compromission (pas systématique), et **authentification multi-facteurs (MFA)** comme priorité absolue pour les accès sensibles. Ce modèle Word, développé par **Ayi NE**, consultant cybersécurité Lead Implementer ISO 27001, intègre ces évolutions doctrinales tout en restant conforme aux exigences ISO 27001:2022, et couvre les règles différenciées par profil d'utilisateur : comptes standards, comptes administrateurs, comptes à privilèges, comptes de service, et comptes invités. La
