

MODÈLE

Modèle de politique de mots de passe & MFA

Politique interne prête à l'emploi, alignée ANSSI / NIST — à personnaliser

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture 11 min Édition 2026 sedona-ai.com

Ce document est une politique interne rédigée pour être adoptée telle quelle : copiez-la, remplacez les champs entre crochets ([Société], [Date], [Responsable]...), faites-la valider par votre direction et diffusez-la. Elle traduit en clauses opérationnelles les recommandations de la CNIL (délibération n° 2022-100), le guide ANSSI/CNIL sur l'authentification et les mots de passe (ANSSI-PG-078), et l'état de l'art international du NIST (SP 800-63B). Le fil directeur reflète la doctrine actuelle : privilégier la longueur sur la complexité, abandonner le renouvellement périodique systématique, généraliser l'authentification multifacteur et réserver le MFA résistant au phishing (FIDO2) aux comptes sensibles. Chaque règle chiffrée renvoie à sa source primaire.

À retenir

- Longueur avant complexité : un mot de passe seul doit atteindre ~80 bits d'entropie (CNIL) — 12 caractères mêlant 4 types, 14 caractères sans spéciaux, ou une phrase de 7 mots.
- Fin du renouvellement périodique systématique pour les comptes standards : on ne change qu'en cas de suspicion de compromission (le renouvellement reste conseillé pour les comptes à privilèges).
- MFA obligatoire sur messagerie, accès distants/VPN, administration et services exposés ; le SMS est le niveau minimal acceptable, à éviter pour les comptes sensibles.
- MFA résistant au phishing de type FIDO2/WebAuthn imposé sur les comptes à privilèges ; la recommandation MFA de la CNIL (délibération n° 2025-019 du 20 mars 2025) est en vigueur et vérifiée en contrôle.
- Ce modèle est un socle à personnaliser et faire valider : les seuils CNIL/ANSSI sont opposables en France, NIST venant en complément international.

01 Comment utiliser ce modèle

Champs à personnaliser

Remplacez systématiquement : [Société] (raison sociale), [Date] (date d'entrée en vigueur), [Responsable] (DSI, RSSI ou dirigeant garant), [Comité] (instance de validation), [Outil MDP] (gestionnaire de mots de passe retenu) et [Contact sécurité] (adresse de signalement d'incident). Adaptez les seuils uniquement à la hausse : les valeurs proposées sont des minima.

Ce modèle a valeur d'exemple à adapter à votre contexte. Il ne se substitue pas à un accompagnement juridique ou à un audit de sécurité. Une fois personnalisé, faites-le adopter formellement (note de service, annexe au règlement intérieur ou à la charte informatique) pour lui donner une portée opposable aux collaborateurs.

02 Article 1 — Objet et périmètre

La présente politique définit les règles applicables au sein de [Société] en matière de mots de passe et d'authentification multifacteur (MFA). Elle vise à protéger l'accès aux systèmes d'information, aux données et aux services de l'organisation contre les accès non autorisés, l'usurpation d'identité et la compromission d'identifiants.

Elle s'applique à l'ensemble des personnes disposant d'un accès aux ressources numériques de [Société] : salariés, dirigeants, stagiaires, intérimaires, prestataires et partenaires. Elle couvre tous les comptes d'accès : comptes utilisateurs, comptes à privilèges (administration), comptes de service et techniques, ainsi que les accès aux services hébergés (SaaS, cloud) utilisés dans le cadre professionnel.

Le respect de cette politique est une condition d'usage des systèmes d'information de [Société]. Elle entre en vigueur le [Date] et est placée sous la responsabilité de [Responsable].

Base réglementaire

Cette politique s'appuie sur la recommandation de la CNIL relative aux mots de passe et autres secrets partagés (délibération n° 2022-100 du 21 juillet 2022), sur le guide ANSSI/CNIL relatif à l'authentification multifacteur et aux mots de passe (ANSSI-PG-078, 2021), sur la recommandation de la CNIL relative à l'authentification multifacteur (délibération n° 2025-019 du 20 mars 2025), et intègre l'état de l'art du référentiel NIST SP 800-63B à titre de complément international non contraignant en France.

03 Article 2 — Principes directeurs

La politique de [Société] repose sur les principes suivants, conformes à la doctrine actuelle de la CNIL, de l'ANSSI et du NIST :

1. Longueur avant complexité. Un mot de passe long est plus résistant qu'un mot de passe court truffé de caractères spéciaux difficiles à mémoriser. La longueur est le premier critère de robustesse.
2. Phrases de passe encouragées. L'usage d'une phrase de passe (suite de mots) est recommandé pour concilier robustesse et mémorisation.
3. Pas de renouvellement périodique systématique. Pour les comptes standards, le changement forcé à intervalle régulier n'est plus imposé ; il n'intervient qu'en cas de suspicion ou de preuve de compromission.
4. Unicité par service. Chaque compte doit avoir un mot de passe distinct : la réutilisation d'un même mot de passe sur plusieurs services est interdite.
5. Liste de mots de passe interdits (blocklist). Les mots de passe trop courants, précédemment compromis ou dérivés du contexte (nom de l'entreprise, prénom, date) doivent être refusés à la création.
6. Gestionnaire de mots de passe recommandé. L'usage de l'outil [Outil MDP] est autorisé et recommandé pour générer et conserver des mots de passe longs et uniques.
7. Authentification renforcée. Le mot de passe seul ne suffit pas pour les accès sensibles : le MFA est généralisé selon l'article 4.

8. Stockage sécurisé. Aucun mot de passe n'est stocké ni transmis en clair, ni ne doit apparaître dans les journaux techniques.

Recommandation NIST

Le référentiel NIST SP 800-63B (révision 4, 2025) formalise cet état de l'art : privilégier la longueur, interdire les règles de composition arbitraires, interdire le renouvellement périodique sauf compromission, comparer tout nouveau mot de passe à une liste de valeurs compromises, et autoriser le copier-coller ainsi que l'affichage temporaire du mot de passe pour faciliter la saisie.

Recommandation CNIL

La CNIL recommande depuis 2022 de ne plus imposer le renouvellement périodique des mots de passe pour les comptes standards, car les changements forcés conduisent à des modifications prévisibles qui affaiblissent la sécurité réelle. Le renouvellement reste conseillé pour les comptes à privilèges.

04 Article 3 — Règles applicables aux mots de passe

Les mots de passe respectent les longueurs minimales suivantes, définies par type de compte. Lorsque le mot de passe est le seul moyen d'authentification (sans MFA ni mesure complémentaire), la CNIL exige une entropie d'au moins 80 bits, atteinte par l'une des trois configurations équivalentes ci-dessous.

Configuration (mot de passe seul, ~80 bits)	Exigence minimale CNIL
Avec 4 types de caractères (majuscules, minuscules, chiffres, spéciaux)	12 caractères minimum
Avec 3 types (majuscules, minuscules, chiffres, sans caractère spécial)	14 caractères minimum
Phrase de passe (suite de mots)	7 mots minimum

80 bits

Entropie minimale exigée par la CNIL quand le mot de passe est le seul moyen d'authentification
CNIL — Délibération n° 2022-100 (2022)

Longueurs minimales retenues par [Société] selon le type de compte :

Type de compte	Longueur minimale	MFA	Renouvellement
Compte utilisateur standard	12 caractères (4 types) ou 14 (3 types) ou phrase de 7 mots	Obligatoire sur les accès listés à l'article 4	En cas de suspicion de compromission uniquement
Compte à privilèges / administrateur	Supérieure au minimum standard ; phrase de passe longue recommandée	Obligatoire, résistant au phishing (FIDO2)	Périodique + immédiat en cas de doute
Compte de service / technique	Secret long généré aléatoirement, stocké dans un coffre-fort	Sans objet (non interactif) ; accès protégé par ailleurs	À la rotation planifiée et en cas de départ d'un détenteur

Recommandation NIST

NIST SP 800-63B-4 impose aux systèmes d'accepter au minimum 8 caractères et recommande 15 caractères minimum lorsque le mot de passe est le seul facteur ; les systèmes doivent supporter des mots de passe d'au moins 64 caractères et ne pas appliquer de règles de composition imposées. Ces valeurs sont des planchers de compatibilité technique : les seuils CNIL (12/14 caractères ou 7 mots) restent la référence opposable en France.

- La réutilisation d'un mot de passe entre plusieurs services (professionnels ou personnels) est proscrite.
- Les mots de passe par défaut (constructeur, éditeur, comptes d'installation) sont changés avant toute mise en service.
- Aucun mot de passe n'est stocké en clair : les systèmes de [Société] les transforment via une fonction cryptographique non réversible avec sel ou clé.
- Le partage d'un mot de passe entre plusieurs personnes est interdit ; chaque accès est nominatif.
- Aucun mot de passe n'est transmis en clair (courriel, message, papier) ni consigné dans un fichier non chiffré.

Recommandation CNIL

La CNIL cite Argon2 et scrypt comme fonctions de hachage adaptées pour le stockage des mots de passe, toujours avec sel ou clé. Les identifiants et mots de passe non reconnus ne doivent jamais apparaître dans les journaux techniques.

05 Article 4 — Authentification multifacteur (MFA)

L'authentification multifacteur combine au moins deux facteurs de nature différente (ce que l'on connaît, ce que l'on possède, ce que l'on est). Elle protège les accès même en cas de vol du mot de passe. Le MFA est obligatoire, dans [Société], sur les accès suivants :

- la messagerie professionnelle (webmail et clients de messagerie) ;
- les accès distants : VPN, bureau à distance (RDP), connexions depuis l'extérieur ;
- les comptes d'administration et d'infrastructure ;

- les applications et services exposés sur Internet (SaaS métier, outils cloud, espaces d'administration) ;
- toute application manipulant des données sensibles ou personnelles.

Les méthodes de MFA autorisées suivent une hiérarchie de robustesse. [Société] privilégie systématiquement la méthode la plus forte disponible pour chaque service.

Méthode MFA	Niveau de sécurité	Usage dans [Société]
Clé physique FIDO2 / WebAuthn	Le plus robuste — résistant au phishing, vérification cryptographique locale	Obligatoire pour les comptes à privilèges ; recommandé pour tous
Application d'authentification (code à usage unique hors réseau téléphonique)	Bon compromis	Acceptée pour les comptes standards
Code par SMS ou appel vocal	Le plus faible — vulnérable au SIM swapping et à l'interception	Niveau minimal acceptable ; à éviter pour les comptes sensibles

Limites du SMS OTP

Le code reçu par SMS reste préférable à un simple mot de passe, mais il constitue le maillon faible du MFA : il est vulnérable au SIM swapping (détournement de la carte SIM) et à l'interception. Le NIST classe l'authentification par SMS ou appel vocal comme « authentificateur restreint ». [Société] réserve le SMS aux services qui ne proposent aucune alternative et l'interdit pour les comptes à privilèges.

MFA résistant au phishing pour les comptes sensibles

Pour les comptes à privilèges et les accès les plus critiques, [Société] impose un authentificateur résistant au phishing de type FIDO2 / WebAuthn (clé physique). Cette technologie vérifie cryptographiquement l'authenticité du service et neutralise les attaques par hameçonnage et par relais.

Recommandation ANSSI / CNIL

L'ANSSI et la CNIL recommandent d'activer le MFA en priorité sur les accès à privilèges, les accès distants, la messagerie et les services exposés sur Internet. La CNIL a adopté le 20 mars 2025 sa recommandation relative à l'authentification multifacteur (délibération n° 2025-019), dont le respect est vérifié dans ses contrôles depuis 2026 ; [Société] s'y conforme.

06 Article 5 — Comptes à privilèges et comptes de service

Les comptes à privilèges (administrateurs système, réseau, applications) et les comptes de service (comptes techniques non interactifs utilisés par des applications ou des automatismes) font l'objet de règles renforcées, car leur compromission a l'impact le plus élevé.

Comptes à privilèges :

- MFA résistant au phishing (FIDO2) obligatoire ;
- mot de passe ou phrase de passe de longueur supérieure au minimum standard ;
- renouvellement périodique maintenu, et changement immédiat en cas de suspicion de compromission ;
- séparation des usages : un administrateur dispose d'un compte nominatif standard pour la bureautique et d'un compte distinct dédié aux tâches d'administration ;
- traçabilité : les connexions aux comptes à privilèges sont journalisées, sans jamais consigner le secret.

Comptes de service et techniques :

- secret long généré aléatoirement, conservé dans un coffre-fort à secrets et jamais codé en dur dans les fichiers de configuration ni les dépôts de code ;
- un compte de service par usage, avec le strict minimum de droits nécessaires (moindre privilège) ;
- rotation planifiée des secrets et rotation immédiate au départ de tout détenteur ayant pu en avoir connaissance ;
- interdiction d'utiliser un compte de service pour une connexion interactive humaine.

Ne pas généraliser l'absence de renouvellement

L'abandon du renouvellement périodique vaut pour les comptes standards. Pour les comptes à privilèges, la doctrine reste plus stricte : le renouvellement régulier est maintenu, et tout mot de passe est changé sans délai en cas de suspicion de compromission, quel que soit le type de compte.

07 Article 6 — Sensibilisation et gestion des exceptions

Sensibilisation. [Société] informe et forme régulièrement ses collaborateurs sur les bonnes pratiques : construction d'une phrase de passe, usage du gestionnaire [Outil MDP], reconnaissance des tentatives d'hameçonnage visant à voler mot de passe ou code MFA, et procédure de signalement. Une session de sensibilisation est intégrée au parcours d'intégration de tout nouvel arrivant.

Signalement. Tout collaborateur qui suspecte la compromission d'un mot de passe ou d'un compte le signale immédiatement à [Contact sécurité] et change son mot de passe sans délai.

Exceptions. Une dérogation à la présente politique (par exemple un système hérité incapable de supporter le MFA ou la longueur requise) ne peut être accordée que par [Responsable], sur demande écrite motivée. Chaque exception est :

1. formalisée par écrit avec sa justification et sa durée de validité ;
2. assortie de mesures compensatoires (restriction d'accès, surveillance renforcée, cloisonnement réseau) ;
3. consignée dans un registre des dérogations tenu par [Responsable] ;
4. réexaminée à échéance, l'objectif étant de résorber l'exception dès que possible.

Mesures complémentaires et seuils

La CNIL admet des exigences d'entropie moindres lorsque des mesures complémentaires existent (temporisation entre tentatives, blocage de compte après plusieurs échecs, détention d'un matériel). [Société] met en œuvre ces protections (verrouillage progressif, limitation du nombre d'essais) sur ses services d'authentification.

08 Article 7 — Sanctions et conformité

Le respect de la présente politique s'impose à toute personne disposant d'un accès aux systèmes de [Société]. Le non-respect délibéré (partage de mot de passe, contournement du MFA, désactivation d'une protection) peut donner lieu aux mesures prévues par le règlement intérieur et la charte informatique, le cas échéant disciplinaires, sans préjudice des recours légaux en cas de dommage.

Conformité réglementaire. Cette politique participe au respect des obligations de sécurité pesant sur [Société] au titre du RGPD (sécurité des traitements de données personnelles, article 32) et, le cas échéant, de la transposition en droit français de la directive NIS2 pour les entités concernées. Elle est cohérente avec les recommandations de la CNIL et de l'ANSSI, autorités de référence en France.

NIST : un complément, pas une obligation française

Le référentiel NIST SP 800-63B est cité comme état de l'art international. Il ne constitue pas une obligation réglementaire en France : les sources primaires opposables restent la CNIL (au titre du RGPD) et l'ANSSI. NIST est mobilisé ici pour renforcer les bonnes pratiques, non comme norme applicable.

09 Article 8 — Entrée en vigueur et révision

La présente politique entre en vigueur le [Date]. Elle est réexaminée au moins une fois par an par [Responsable] (ou [Comité]) et à chaque évolution significative : nouvelle recommandation de la CNIL ou de l'ANSSI, incident de sécurité, changement d'outillage ou d'organisation. Toute révision est datée, versionnée et communiquée à l'ensemble des personnes concernées.

Version	Date	Rédacteur / Responsable	Nature de la révision
1.0	[Date]	[Responsable]	Version initiale

Adoptée le [Date] — [Société] — Responsable : [Responsable].

10 Aller plus loin avec Sedona.AI

Une politique n'a de valeur que si elle est appliquée et vérifiée sur le terrain. Sedona.AI accompagne les PME et ETI françaises sur trois volets complémentaires :

- Audit de surface et OSINT — repérer les mots de passe apparus dans des fuites, les services d'administration ouverts sur Internet et les points d'entrée non protégés par MFA.

- Sensibilisation et exercices de phishing — mesurer et renforcer la vigilance des équipes face au vol de mots de passe et de codes MFA.
- Sedona Radar — un audit de sécurité externe automatisé : il analyse ce que votre domaine expose sur Internet et donne des indicateurs de maturité sur six référentiels (NIS2, RGPD, ISO 27001, ANSSI Hygiène, OWASP Top 10, Cadre Sedona, grille propre à Sedona qui n'est pas un référentiel de l'ANSSI).

Précision d'honnêteté

Sedona Radar donne des indicateurs de maturité (dont NIS2) ; il ne certifie rien, et il n'existe aucune certification NIS2. Sedona.AI n'est ni qualifiée PASSI ni certifiée ISO 27001.

§ Sources

1. ANSSI-PG-078 — Recommandations authentification multifacteur et mots de passe (ANSSI/CNIL, 2021) — <https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe>
2. CNIL / Légifrance — Délibération n° 2022-100 du 21 juillet 2022 — <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046432885>
3. CNIL — Mots de passe : recommandations pour maîtriser sa sécurité (2022) — <https://www.cnil.fr/fr/mots-de-passe-recommandations-pour-maitriser-sa-securite>
4. CNIL — Délibération n° 2025-019 du 20 mars 2025, recommandation relative à l'authentification multifacteur — <https://www.cnil.fr/fr/authentification-multifacteur>
5. NIST — SP 800-63B-4 Digital Identity Guidelines (2025) — <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf>
6. NIST — SP 800-63B (page HTML de référence) — <https://pages.nist.gov/800-63-3/sp800-63b.html>
7. Cybermalveillance.gouv.fr — La double authentification — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification>

Des adresses de votre domaine apparaissent-elles dans des fuites ?

Sedona Radar recherche les adresses e-mail de votre domaine dans des fuites de données publiques, et donne des indicateurs de maturité sur six référentiels dont NIS2 et ANSSI Hygiène. Lancez un scan gratuit pour voir ce que votre domaine expose.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit