POLITIQUE MOTS DE PASSE ENTREPRISE

Règles de gestion des mots de passe — Applicable à tous les collaborateurs

POLITIQUE INTERNE À DIFFUSER AUX SALARIÉS

12
caractères minimum
Pour tout mot de passe utilisateur standard

16
caractères minimum
Comptes administrateurs et accès privilégiés

4
types de caractères
Maj + min + chiffres + caractères spéciaux

0
réutilisation
Jamais le même mot de passe sur deux services

MFA
Multi-facteurs
Obligatoire sur tous les accès distants et sensibles

À FAIRE

- ✓ Utiliser un gestionnaire de mots de passe
- ✓ Créer des mots de passe aléatoires et longs
- ✓ Activer la double authentification (MFA)
- ✓ Changer son mot de passe dès suspicion de compromission
- ✓ Utiliser une phrase de passe mémorisable (ex. : "Cheval!Batterie.Agrafe$Éclair")
- ✓ Vérifier ses comptes sur haveibeenpwned.com

INTERDIT

- ✗ Partager son mot de passe (même à son responsable)
- ✗ Utiliser des mots de passe évidents (prénom, date de naissance, "123456")
- ✗ Réutiliser le même mot de passe sur plusieurs services
- ✗ Écrire son mot de passe sur un post-it ou dans un fichier non chiffré
- ✗ Enregistrer dans le navigateur sans gestionnaire sécurisé
- ✗ Transmettre un mot de passe par email ou SMS

RÈGLES PAR NIVEAU D'ACCÈS

Niveau d'accès	Longueur min.	Complexité	Renouvellement	MFA	Gestionnaire
Standard (utilisateur)	12 caractères	Maj + min + chiffre + spécial	Tous les 90 j.	Recommandé	Fortement conseillé
Administrateur IT	16 caractères	Aléatoire complet	Tous les 60 j.	**Obligatoire**	Obligatoire
Critique (RH, finance, direction)	20 caractères	Généré par gestionnaire	Tous les 30 j.	**Obligatoire**	Obligatoire
Super administrateur / Root	24 caractères	Totalement aléatoire	Après chaque usage	**Obligatoire (matériel)**	Coffre-fort dédié

BLOCAGE AUTOMATIQUE : Tout compte est automatiquement verrouillé après 5 tentatives de connexion erronées. Contacter le service IT pour déverrouillage.

AUTHENTIFICATION MULTI-FACTEURS (MFA / 2FA)

MÉTHODE MFA	USAGE	RECOMMANDÉ POUR
Application authenticator (TOTP)	Code à 6 chiffres renouvelé toutes les 30 s.	Tous les utilisateurs — Niveau Standard minimum
Clé de sécurité physique (FIDO2/YubiKey)	Clé matérielle, résistante au phishing	Administrateurs, accès critiques — Niveau Élevé
SMS (OTP)	Code envoyé par SMS	Toléré uniquement si autre méthode non disponible
Email OTP	Code envoyé par email	Déconseillé — en dernier recours uniquement

GESTIONNAIRES DE MOT DE PASSE RECOMMANDÉS

Bitwarden

Open source — Cloud — Self-hosted

- › Gratuit individuel, abordable équipe
- › Partage en équipe / coffre partagé
- › Audit de sécurité intégré

RECOMMANDÉ

KeePass / KeePassXC

Open source — Local uniquement

- › 100% gratuit et open source
- › Stockage local (pas de cloud)
- › Contrôle total des données

GRATUIT

1Password

Commercial — Cloud sécurisé

- › Ergonomie excellente
- › Fonctionnalités équipes avancées
- › Rapports de sécurité détaillés
- › Clé secrète pour protection renforcée

ENTREPRISE

PROCÉDURE EN CAS DE COMPROMISSION

1. Changer **immédiatement** le mot de passe du compte compromis
2. Vérifier tous les autres comptes utilisant le même mot de passe
3. Activer ou renforcer le MFA sur tous les comptes sensibles
4. Alerter le service IT / RSSI sans délai
5. Vérifier les activités récentes suspectes sur les comptes
6. Enregistrer l'incident dans le registre des incidents
7. Si données personnelles concernées : alerter le DPO (72h CNIL)

LIENS UTILES

- › Vérifier si vos données ont été compromises : **haveibeenpwned.com**

- Guide ANSSI sur les mots de passe : **ssi.gouv.fr**
- Délibération CNIL sur les mots de passe : **cnil.fr/mots-de-passe**
- Télécharger Bitwarden : **bitwarden.com**

Besoin d'un accompagnement pour déployer une politique de mots de passe dans votre entreprise ?
ayinedjimi-consultants.fr/contact