POlitique de Mots de passe

 Modèle

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents**  |  |
| Auteur  |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par  |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date d'approbation** | **Approuvé par**  | **Description du changement** |
| 1.0 |  |  |  |

# Intro

Les mots de passe sont souvent utilisés pour authentifier les utilisateurs. Ce document fournit une politique pour l'utilisation et la mise en œuvre des mots de passe pour les systèmes d'information confidentiels et critiques.

Nous avions l'habitude de penser que la meilleure façon de sécuriser les mots de passe était de les rendre forts et de les changer souvent. Aujourd'hui, la nouvelle philosophie qui consiste à rendre les mots de passe longs mais conviviaux gagne en popularité. L'authentification multifactorielle est fortement encouragée et devrait être utilisée chaque fois que possible, non seulement pour les comptes liés au travail, mais aussi pour les comptes personnels.

Ce document fait partie d'un ensemble de documents qui aident l**'[Organisation]** à établir une stratégie solide en matière de cybersécurité.

# Paramètres du mot de passe

## Force du mot de passe

La force du mot de passe est importante pour réduire les risques d'abus.

Les systèmes de mots de passe doivent imposer l'utilisation de mots de passe forts conformément à ces règles :

* La longueur minimale autorisée du mot de passe doit être respectée **(minimum X caractères, X est recommandé).**
* Les mots de passe des administrateurs doivent contenir au moins **XX** caractères.
* Les mots de passe des comptes de service doivent comporter au moins **XX** caractères.
* Les mots de passe très longs devraient être autorisés (par exemple 256 caractères).
* Les mots de passe contenant votre nom d'utilisateur doivent être rejetés
* Les mots de passe contenant votre nom ou votre prénom doivent être rejetés.
* Des mots de passe complexes doivent être appliqués, contenant au moins trois des catégories suivantes :
	+ - Lettres majuscules (A-Z)
		- Minuscules (a-z)
		- Chiffres (0-9)
		- Caractères spéciaux : !@#$%^&\*() etc

Exceptions :

Dans les cas suivants, un mot de passe d'au moins 4 chiffres est autorisé :

* Si le code est un ajout à un identifiant d'accès physique tel qu'une carte à puce ou un jeton
* Si le système n'est pas connecté à un réseau et qu'il dispose de contrôles de sécurité physiques solides
* Pour déverrouiller l'écran d'un appareil mobile **[Organisation]** tel qu'un smartphone ou une tablette

## Politique de changement de mot de passe

Pour réduire le risque de compromission des mots de passe, il convient de les modifier régulièrement. Les règles suivantes s'appliquent :

* Les mots de passe par défaut des nouveaux appareils doivent être modifiés.
* Les systèmes doivent permettre aux utilisateurs de changer de mot de passe à tout moment.
* Le changement périodique de mot de passe doit être imposé en fonction de la longueur minimale du mot de passe imposée par le système.
* Lorsque la longueur minimale autorisée du mot de passe du système est de **X** caractères, les utilisateurs doivent être contraints de changer de mot de passe tous les **X** mois (ou **XX** jours).
* Lorsque la longueur minimale autorisée du mot de passe du système est de **XX** caractères, les utilisateurs doivent être contraints de changer de mot de passe tous les **X** mois (ou **XX** jours).
* Les mots de passe fournis par d'autres personnes que l'utilisateur lui-même (par exemple, le département TIC) doivent être modifiés lors de la première connexion.
* Les systèmes de mots de passe doivent explicitement interdire la réutilisation des **X** derniers mots de passe au moins.
* Les mots de passe partagés connus des personnes qui quittent l'organisation doivent être modifiés.

Exceptions :

La politique de changement des mots de passe est recommandée mais non obligatoire dans les cas suivants :

* Si le mot de passe est utilisé pour un compte de service et ne peut pas être utilisé pour une connexion interactive
* Si le code est un ajout à un identifiant d'accès physique tel qu'une carte à puce ou un jeton
* Si le système n'est pas connecté à un réseau et qu'il dispose de contrôles de sécurité physiques solides
* Pour déverrouiller l'écran d'un appareil mobile **[Organisation]** tel qu'un smartphone ou une tablette

## Prévention des attaques

Les systèmes doivent comporter au moins un mécanisme de prévention des attaques par force brute. Voici quelques exemples de ces techniques :

* **verrouillage du compte :**
Une politique d'exclusion désactive la fonctionnalité de connexion pour un compte spécifique. (par exemple, verrouiller le compte pendant **XX** minutes après **X** échecs de connexion).
* **Liste noire d'adresses IP** :
Comme les politiques de blocage de compte, ce mécanisme détecte les tentatives de connexion infructueuses, mais il vérifie les adresses IP d'où proviennent les demandes de connexion. Si un trop grand nombre de tentatives est détecté (par exemple 20) à partir d'une adresse IP donnée, cette adresse est inscrite sur une liste noire.
* **Délai de connexion :**Ce mécanisme ajoute un délai de répétition incrémentiel après l'utilisation d'un mot de passe incorrect. (par exemple, attendre 0,5 seconde après deux tentatives infructueuses, 1 seconde après le troisième échec, 2 secondes après le quatrième, 4 secondes après le cinquième, etc.)

# Protection par mot de passe

* Les mots de passe ne doivent être communiqués à personne, y compris aux supérieurs hiérarchiques et aux collègues. Tous les mots de passe doivent être traités comme des informations sensibles et confidentielles de **[Organisation**]
* Les mots de passe ne doivent pas être inclus dans des messages électroniques ou d'autres formes de communication électronique, ni communiqués à quiconque par téléphone.
* Les mots de passe ne doivent être stockés que dans des gestionnaires de mots de passe autorisés par l'organisation. Les mots de passe sur papier doivent être évités, à moins qu'il n'y ait une sécurité physique forte (comme un coffre-fort).
* N'utilisez pas la fonction "Mémoriser le mot de passe" des applications (par exemple, les navigateurs web).
* Toute personne qui soupçonne que son mot de passe a été compromis doit le signaler et changer tous les mots de passe pertinents.

## Distribution par courrier électronique

La distribution de noms d'utilisateur et de mots de passe par courrier électronique peut s'avérer efficace et pratique. Bien que le courrier électronique ne soit pas le moyen de communication le plus sûr par défaut, il peut être utilisé dans les cas suivants :

* Aucun système de courrier électronique externe n'est utilisé.
* Le courrier électronique est envoyé de manière cryptée (comme Office 365)
* La combinaison spécifiée du nom d'utilisateur et du mot de passe expire après la première utilisation ou, si elle n'est pas utilisée, après **1 mois.**

## Distribution par SMS

Le SMS n'est pas un protocole sécurisé et ne doit jamais être utilisé pour envoyer des combinaisons de noms d'utilisateur et de mots de passe. Il peut être utilisé pour envoyer des informations de connexion partielles, mais uniquement si les conditions suivantes sont remplies :

* Le message ne contient au maximum qu'une partie de la combinaison : système, nom d'utilisateur, mot de passe ou jeton. Les autres parties sont envoyées via d'autres méthodes de distribution.
* L'utilisateur s'attend à recevoir le message et est donc susceptible de l'utiliser bientôt.
* Les informations contenues dans le message expirent après la première utilisation ou, si elles ne sont pas utilisées, après un mois.