T-NSA-810 - CIA

Politique des mots de passe

Historique des versions du document			
Version	**Auteur**	**Raison de la modification**	**Date**
v1.0	Alisson CARMONA	Création initiale du document	04/07/24

Introduction

Dans ce projet, la sécurité des informations est une priorité absolue. La fragilité des mots de passe des VMs ayant été détectée très rapidement, il est important d'établir une protection par mot de passe robuste. Celle-ci constituera une première ligne de défense contre les accès non autorisés.
Conformément aux recommandations de la **CNIL** (Commission Nationale de l'Informatique et des Libertés) et de l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information), cette politique des mots de passe vise à garantir un niveau de sécurité élevé pour tous les utilisateurs au sein du projet.

I. Exigences générales

Tous les utilisateurs doivent créer des mots de passe conformément aux critères suivants, en optant pour une de ces 3 options :

- **Option 1, le mot de passe "complexe" :**
  - Longueur minimale de 12 caractères
  - Doit inclure des lettres majuscules et minuscules
  - Doit inclure des chiffres
  - Doit inclure des caractères spéciaux choisis parmi une liste d'au moins 37 caractères spéciaux

- **Option 2, le mot de passe "standard" :**

    - Longueur minimale de 14 caractères
    - Doit inclure des lettres majuscules et minuscules
    - Doit inclure des chiffres
    - Aucun caractère spécial requis

- **Option 3, l'utilisation d'une passphrase :**
    - Doit être composée d'au moins 7 mots
    - Les mots doivent être suffisamment longs et non triviaux pour assurer une robustesse adéquate

II. Règles de création et de modification des mots de passe

1. Les mots de passe doivent être créés de manière à éviter toute ressemblance avec des informations personnelles.
2. Chaque mot de passe doit avoir une seule utilisation/fonction au sein du projet.
3. En cas de modification de mot de passe utilisé par plusieurs personnes du projet, celui-ci doit être communiqué, puis le message doit être détruit une fois la modification prise en compte par tout le monde.

III. Règles de stockage et de gestion des mots de passe

1. Les mots de passe doivent être mémorisés et ne doivent jamais être notés sur des supports non sécurisés (post-it, feuille, carnet, bloc-note virtuel…).
2. Il est obligatoire d'utiliser un gestionnaire de mots de passe sécurisé pour stocker et gérer les différents mots de passe du projet.
3. Les mots de passe ne doivent pas être partagés avec d'autres personnes et le besoin d'en connaître doit s'appliquer.

IV. Procédure en cas de compromission

En cas de suspicion de compromission d'un mot de passe, l'utilisateur doit le changer immédiatement et signaler l'incident à l'administrateur système (ou à la personne référente).

Les mots de passe compromis doivent être réinitialisés et les utilisateurs doivent être informés des mesures à prendre pour renforcer la sécurité de leurs comptes.

V. Bonnes pratiques supplémentaires à appliquer (optionnel)

Il est recommandé d’activer l'authentification multi-facteurs (MFA) lorsqu'elle est disponible, pour une sécurité renforcée.

Il est également recommandé de ne pas utiliser les mêmes mots de passe pour différents services ou comptes, sauf si un besoin légitime est identifié.

Conclusion

L'application stricte de cette politique de mot de passe est nécessaire pour protéger nos informations et nos systèmes contre tout accès non autorisé. Tous les utilisateurs sont tenus de se conformer à ces directives pour garantir un environnement sûr et digne de confiance.

Pour toute question ou assistance concernant cette politique de mot de passe, veuillez contacter votre administrateur informatique ou votre service informatique dédié.