Centre opérationnel en cyberdéfense
Ministère de l'Éducation et
ministère de l'Enseignement supérieur

Règles de sécurité associées à la gestion des mots de passe

Les règles de sécurité

Les règles de sécurité associées à la gestion des mots de passe sont des paramètres déployés par les services informatiques d'une organisation pour guider les utilisateurs dans le choix de mots de passe sécuritaire.

Le mot de passe

Le mot de passe d'un utilisateur (personnel administratif, personnel enseignant, étudiant, etc.) constitue un paramètre important dans la stratégie de défense d'une organisation.

La notion de complexité

Le mot de passe doit être composé d'un certain nombre d'éléments, tel qu'énumérés ci-dessous :

- **Lettres majuscules**
- **Lettres minuscules**
- **Chiffres**
- **Caractères spéciaux :** (ex : @, ?, #, $, %, ^, &)

La notion de complexité est respectée lorsque le mot de passe contient au moins trois de ces quatre éléments.

Afin d'outiller les utilisateurs dans le choix d'un mot de passe sécuritaire ou plus robuste, voici des **règles minimales** à appliquer dans vos organisations :

Règles de sécurité pour les élèves et étudiants

- Longueur du mot de passe : 8 caractères
- Intégration dans le mot de passe de critères de complexité : 3
- Réinitialisation des mots de passe : 1 fois par année
- Verrouillage du compte après 10 tentatives infructueuses
- Conservation de l'historique des mots de passe : les 6 derniers

Règles de sécurité pour l'ensemble du personnel

- Longueur du mot de passe : 8 caractères
- Intégration dans le mot de passe de critères de complexité : 3
- Réinitialisation des mots de passe : 4 fois par année
- Verrouillage du compte après 6 tentatives infructueuses
- Conservation de l'historique des mots de passe : les 10 derniers

Règles de sécurité pour les comptes avec privilèges

- Longueur du mot de passe : 12 caractères
- Intégration dans le mot de passe de critères de complexité : 3
- Réinitialisation des mots de passe : 4 fois par année
- Verrouillage du compte après 3 tentatives infructueuses
- Intégration d'une authentification multifacteur (ex : Microsoft Authenticator, clé ou jeton RSA)

Quelques conseils pour vos utilisateurs

Il faut retenir (mémoriser) son mot de passe. Il ne faut pas l'écrire. L'utilisation d'un trousseau d'accès chiffré est une bonne option. Utilisez une phrase, c'est plus facile à retenir! Pensez à substituer certains caractères de votre mot de passe (ex : changer certaines lettres pour des chiffres et des caractères spéciaux qui leur ressemblent). Ne pas utiliser des informations permettant de vous identifier (ex : votre nom, prénom, votre identifiant, adresse civique).

Outils technologiques (à titre indicatif)

Outil de test de la robustesse de mot de passe de l'éditeur Kaspersky

Logiciel de gestion de mot de passe : https://keepass.info/