Source cybermalveillance.gouv.fr

Respecter la recommandation de la CNIL dans le cas d'une authentification des utilisateurs basée sur des mots de passe, notamment en stockant les mots de passe de façon sécurisée et en appliquant les règles de complexité suivantes pour le mot de passe :

- **au moins 8 caractères** comportant 3 des 4 types de caractères (majuscules, minuscules, chiffres, caractères spéciaux) si l'authentification prévoit une restriction de l'accès au compte (cas le plus courant) comme :
-
    - une temporisation d'accès au compte après plusieurs échecs ;
    - un « Captcha » ;
    - **un verrouillage du compte après 10 échecs** ;
- 12 caractères minimum et 4 types de caractères si l'authentification repose uniquement sur un mot de passe ;
- plus de 5 caractères si l'authentification comprend une information complémentaire. L'information complémentaire doit utiliser un identifiant confidentiel d'au moins 7 caractères et bloquer le compte à la 5ème tentative infructueuse ;
- le mot de passe peut ne faire que 4 caractères si l'authentification s'appuie sur un matériel détenu par la
- personne et si le mot de passe n'est utilisé que pour déverrouiller le dispositif matériel détenu en propre
- par la personne (par exemple une carte à puce ou téléphone portable) et qui celui-ci se bloque à la 3ème tentative infructueuse.

Des moyens mnémotechniques permettent de créer des mots de passe complexes, par exemple :

- en ne conservant que les premières lettres des mots d'une phrase ;
- en mettant une majuscule si le mot est un nom (ex : Chef) ;
- en gardant des signes de ponctuation (ex : ') ;
- en exprimant les nombres à l'aide des chiffres de 0 à 9 (ex : Un 1) ;
- en utilisant la phonétique (ex : acheté ht).