Plan de Test

Les tests définis garantissent la robustesse et la sécurité du générateur de mots de passe en couvrant plusieurs aspects critiques.

1. Vérification de la longueur du mot de passe

- **Mot de passe court** : Vérifier qu'un mot de passe de 8 caractères est généré correctement.
- **Mot de passe long** : Vérifier qu'un mot de passe de 32 caractères est généré correctement.
- **Longueur invalide** : Tester les valeurs inférieures à 4 et supérieures à 128 pour s'assurer qu'une erreur est renvoyée.

2. Vérification des critères de composition

- **Mot de passe avec uniquement des lettres** : Générer un mot de passe de 12 caractères et vérifier qu'il contient uniquement des lettres (majuscules et minuscules).
- **Mot de passe avec toutes les catégories** : Générer un mot de passe de 16 caractères et vérifier la présence de majuscules, minuscules, chiffres et caractères spéciaux.
- **Mot de passe sans caractères spéciaux** : Générer un mot de passe de 20 caractères et s'assurer qu'il ne contient que des lettres et des chiffres.

3. Vérification de l'unicité et de l'aléatoire

- **Génération successive de mots de passe** : Générer trois mots de passe successivement avec les mêmes paramètres et s'assurer qu'ils sont différents.
- **Comparaison entre sessions** : Relancer l'application et générer un mot de passe avec les mêmes critères, puis vérifier qu'il est différent des précédents.
- **Unicité dans une session** : Générer 1000 mots de passe et vérifier qu'aucun n'est identique.