ANSWERS TO THE 5 QUESTIONS ASKED ARE GIVEN BELOW RESPECTIVELY:

1. Hashing algorithm used here to protect passwords is MD5 which is an outdated password hashing algorithm.
2. MD5 offers very little protection in the event of a password database leaking and is very much prone to collisions.
3. Use a dedicated password hashing algorithm bcrypt, scrypt or PBKDF2 as this will greatly increase the time needed to crack individual passwords.

Implement salting to prevent usage of rainbow tables to speed up cracking.

1. The current password policy is not aligned with industry best practices   
   allowing users to have short passwords (6 characters) and reuse usernames as part of passwords.
2. Increase the minimum password length requirement to 10 characters-this will increase the computational effort required to crack password and will give additional time to change all passwords in the event of the password database being leaked.

Prevent passwords to be the same as usernames or reused as part of the password-such password combination is easy to check without gaining access to the password database itself.