Dear Sir/Madam

I hope you are doing well.   
  
Allow me to extend my gratitude as a governance analyst after conducting an analysis, it was determined that the organization uses an outdated password hashing algorithm (such as MD5) that provides minimal protection in case of a password database attack.

The analysis proposes several improvements to enhance password protection against attacks.

1. MD5 hashing algorithm was used to protect those passwords that provide very little security from the attack. Popular password hashing algorithms include bcrypt, Argon2, and SHA-256. Bcrypt and Argon2 are recommended due to their resistance to brute-force attacks.
2. The level of protection offered by a password hashing mechanism depends on the specific algorithm used. Stronger algorithms like bcrypt and Argon2, along with proper salt and pepper usage, provide robust protection against brute-force and dictionary attacks, making it significantly harder for attackers to recover passwords.
3. Implement strong password hashing bcrypt, unique salts, and a site-wide pepper for added protection. Enforce multi-factor authentication, regularly update passwords, monitor for unusual activity, and encrypt password databases while educating users on security practices to make cracking significantly harder for hackers in the event of a database leak.
4. The organization's password policy includes a minimum password length of 12 characters, mandating a mix of uppercase, lowercase, numbers, and special characters. Passwords cannot be reused, and they expire every 90 days. An account lockout system activates after several failed login attempts, while multi-factor authentication is encouraged for added protection.
5. To enhance password security, require longer and more complex passwords (e.g., "P@ssw0rd!462"), promote two-factor authentication, use account lockout policies, educate users, and periodically review and adapt policies. Employ secure password storage and monitor for suspicious activity. For added safety, we can use third-party services to check for password compromises for instance, Have I Been Pwned.

Thank you for your time and consideration.

Regards,

Taranbeer Singh