Dear Sir/Ma'am,

After trying to crack all the leaked hashes, I found various vulnerabilities in your password policy and this Email concludes all the findings and suggestions to improve your password policy.

All the passwords which are compromised were using MD5 which is weaker and prone to collisions.

It was very easy to crack with rockyou.txt or crackstation wordlist. I would suggest that you use a dedicated password hashing algorithm bcrypt, scrypt or PBKDF2 as this will greatly increase the time needed to crack individual passwords

After cracking the password I found the following things about the organization's password policy:

1. The minimum length for password is set to 6.
2. There is no specific requirement for password creation. Users can use any combination of words and letters to create a password.

You can include several new things in your password policy. My recommendations are:

1. Avoid common words and character combinations in your password
2. Increasing the minimum password length requirement to 10 characters-this will increase the computational effort required to crack passwords and will give additional time to change all passwords in the event of the password database being leaked,
3. Don't reuse your passwords.
4. Implement salting to prevent usage of rainbow tables to speed up cracking
5. Include special characters, Capital and Small letters, and numbers in your password.
6. Do not let users include their username, actual name, date of birth and other personal information while creating a password.
7. Educate users on the benefits of password managers. Having a password manager allows having very long and completely random passwords (e.g. M>?[tk6Cfep6BrZ4J)KZWQ8)) without the need to remember/write down. A strong passphrase is still required as a master key to access the password manager
8. Train your users to follow all these policies.

Thank You Regards

Shubham Trivedi