Dear Sir/Madam,

After trying to crack all the leaked hashes, I found several complications in your password policy and this document concludes all the findings and suggestions to improve your password policy

Secure Hash Algorithm and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication.

All the password 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 very strong password encryption mechanism to create hashes for the password based on SHA.

After cracking the password I found following things about company’s password policy.

* Minimum length for password is normally set to 6
* There is no specific requirement for the purpose creation. Users can use any combination of word and letters to create a password

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

* Avoid common words and character combinations in your password
* Longer passwords are better, 8 characters is a starting point
* Don’t reuse your passwords
* Include special characters ,Capital and Small Letters, numbers in your password
* Do not let users include their username, actual name, date of birth and other personal information while creating a password
* Train you users to follow all these policies

Thank you Regards,

Jaskeerat Singh