Respected Sir/Ma'am:

While researching and cracking passwords , I found several loopholes in your password policy I have researched and tried my level best to improve your password policy.

After the analysis, it was observed that the organization was using an outdated password hashing algorithm i.e. **Message Digest (MD5)** which is a weaker hash algorithm.
It offers very little protection in the event of a password database leaking.

The passwords were very easy to crack from the password cracking tools like Hashcat and Aircrack. Therefore we need to use a very strong password encryption mechanism.

After cracking the passwords, the following things were observed about the organization's password policy:-

1. The minimum length for a password is set to 6 i.e. short passwords.
2. The user can also reuse our usernames to set them as passwords.
3. No specific criteria for the selection of the password i.e. the user can use any combination of words and letters to set their passwords.

As a result of the analysis, these are the recommendations that I feel the organization can include in their policy to increase the overall password protection:-

1. Increase the minimum password length requirement to 10 characters. This will increase the computational effort required to crack the password.
2. Prohibit users from using their date of birth phone numbers and usernames as part of their password as such password combinations are again easy to crack.
3. Include special characters, numbers, and Capital letters in the password.
4. Educate users on the benefit of using password managers. Having a password manager will allow having very long and random passwords(EG: u5@8ekoFq$%gmdosA21wE) without the need to remember them.
5. Train the users to follow the password policies and create safe and easy to remember passwords that are strong and not so easy to crack.

Thank you

Muskaan Mishra
Btech 2nd year (Information Technology)
ADGITM, New Delhi

Security Algorithms used:

experthead:e10adc3949ba59abbe56e057f20f883e – MD5
interestec:25f9e794323b453885f5181f1b624d0b – MD5
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5
simmson56:96e79218965eb72c92a549dd5a330112 – MD5
bookma:25d55ad283aa400af464c76d713c07ad – MD5
popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5
liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5
johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5
flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5
oranolio:16ced47d3fc931483e24933665cded6d - MD5
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5
moodie:8d763385e0476ae208f21bc63956f748 - MD5
nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5
bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5

Cracked Passwords:

experthead:e10adc3949ba59abbe56e057f20f883e - 123456
interestec:25f9e794323b453885f5181f1b624d0b - 123456789
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password
simmson56:96e79218965eb72c92a549dd5a330112 - 111111
bookma:25d55ad283aa400af464c76d713c07ad - 12345678
popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!
liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1
johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered