Dear Sir/Ma’am,

I found several defenselessness after trying to crack all the leaked hashes, in your password policy and this email concludes all the findings and suggestions to improve your password policy. Secure Hash Algorithm (SHA) 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 a weaker hash algorithm and is prone to collisions. It was very easy to crack with Hashcat.com and rockyou.txt wordlist via terminal and web browsers.

Here I have also another website to find password: https://crackstation.net/,

https://hashes.com/en/decrypt/hash,

After cracking the passwords, we find the following things about organization’s password policy:

- Avoid common words and character combinations in your password.
- There is no specific requirement for the password 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:
- Longer passwords are better, 8 characters is a starting point.
- Minimum length for password is set to 6.
- Don’t reuse your passwords.
- Include special character, Capital and Small letters, numbers in your password.
- Don’t let users include their username, actual name, date of birth and other personal information while creating a password.
- Train your users to follow these policies to keep their passwords safe.

Thanking You,

Name: SK WASIM AKROM HOSSAIN

B Tech Electrical Engineering

Observation:

experthead:e10adc3949ba59abbe56e057f20f883e	:	md5	123456
interestec:25f9e794323b453885f5181f1b624d0b	:	md5	123456789
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4	:	md5	qwerty
reallyche:5f4dcc3b5aa765d61d8327deb882cf99	:	md5	password
simmson56:96e79218965eb72c92a549dd5a330112	:	md5	111111
bookma:25d55ad283aa400af464c76d713c07ad	:	md5	12345678
popularkiya7:e99a18c428cb38d5f260853678922e03	:	md5	abc123
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759	:	md5	1234567
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c	:	md5	password1
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98	:	md5	password!
liveltekah:3f230640b78d7e71ac5514e57935eb69	:	md5	qazxsw
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b	:	md5	Pa$$word1
johnwick007:f6a0cb102c62879d397b12b62c092c06	:	md5	bluered

1)What type of hashing algorithm was used to protect passwords?

Ans: Md5

2) What level of protection does the mechanism offer for passwords?

Ans: MD5 is insecure and provides a very low level of protection and should not be used in any application. Users receive a prompt for a username or password before they're given access

3)What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

Ans : Controls to be implemented to make cracking harder:

i) A min-length password rule should be implemented.

ii)Passwords must contain some special characters, numbers, lowercase alphabets as well as upper case alphabets.

iii)Using a hashing algorithm which provides a high level of protection. Example:SHA-256 and SHA-3.

iv) Concept of password salting must be used.

4)What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?
Ans: i)There is no rule regarding the minimum length of the password.

ii)There is no rule regarding use of special characters in the password.

5)What would you change in the password policy to make breaking the passwords harder?
Ans: i) The password must be of minimum 8 characters.

ii) Minimum 2 special characters **(/,#,*,...)** must be used in the password.

iii)An external API based tool which checks for password strength should show that the used password is strong.