Dear Sir/Mam,

After going through all information and learning resources I have come on the conclusion to prevent successful cracking of passwords and potential are as follows:

1) Going through passwords, firstly learned about tools that use to cracked passwords and different methods using resources like kali Linux or websites like hashes.com.

2) Then learned about command line installation of kali Linux and other required tools for cracking password.

3) Then checked the passwords you have provided in terms of Hashes.

4) After copying the hash id to hashes.com and pasted there in a tool name called Identify hashes type then after submitting it gives possible algorithm for example MD5 uses to encrypt the copied password.

5) So then after going to Kali Linux to crack password through virtually.

6) Going on terminal tool used for cracking is Hashcat, so to start cracking and making file after going through options for MD5 hyphen m is used.

7) After checking the wordlist in kali Linux choosing 1 for cracking passwords.

8) So at Finally after setting up everything to crack password now, simply choose any Hash from given list of passwords from task then creating file at wordlist and using command we get the password.

9) Also cracking another method which is going on Crackstation.com pasting non salted hashes and after submitting it shows algorithm type and password.

After performing all above steps there are some vulnerabilities found in your password policy,

Secure Hash Algorithm(SHA) and Message digests(MD) are the standard cryptographies hash functions to provide data security for authentication.

- **Observations are –**

  - All passwords are using same MDs which is weaker and prone to collisions.
  - It was very easy to crack with crack station or with kali Linux wordlist. Simply observation suggest that should use strong password encryption mechanism to create hashes for the password based on SHA.
  - The organization settled their password in 6 digits in their policy.

So for that we can use any no of character and symbols to create passwords as there is no specific criteria or requirement for password creation.

There are some suggestions from my side:

- Avoiding common words, spaces and character in combination instead add some symbols upper case letters and numbers for strong password.
- Longer password is always better.
- Don’t reuse same password again.
- Most important thing doesn’t use personal information in password that lead vulnerability and hacker can access every information.