Respected Sir/Madam

I was able to crack 15 of the 19 hashcodes given to me in the password dump file using https://md5decrypt.com

e10adc3949ba59abbe56e057f20f883e : 123456 MD5
25f9e794323b453885f5181f1b624d0b : 123456789 MD5
d8578edf8458ce06fbc5bb76a58c5ca4 : qwerty MD5
5f4dcc3b5aa765d61d8327deb882cf99 : password MD5
96e79218965eb72c92a549dd5a330112 : 111111 MD5
25d55ad283aa400af464c76d713c07ad : 12345678 MD5
e99a18c428cb38d5f260853678922e03 : abc123 MD5
fcea920f7412b5da7be0cf42b8c93759 : 1234567 MD5
7c6a180b36896a0a8c02787eeafb0e4c : password1 MD5
6c569aabbf7775ef8fc570e228c16b98 : password! MD5
3f230640b78d7e71ac5514e57935eb69 : qazxsw MD5
917eb5e9d6d6bca820922a0c6f7cc28b : Pa$$word1 MD5
f6a0cb102c62879d397b12b62c092c06 : bluered MD5

#Conclusion

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.

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 (/,#,*,... etc) 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.