Analysis and Findings on the given pass_dump.txt file

I have cracked some of the hashed passwords with the help of *2john Hash Extractor and Hashcat tool.

e10adc3949ba59abbe56e057f20f883e:123456
d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
3f230640b78d7e71ac5514e57935eb69:qazxsw
fcea920f7412b5da7be0cf42b8c93759:1234567
f6a0cb102c62879d397b12b62c092c06:bluered
5f4dcc3b5aa765d61d8327deb882cf99:password
8d763385e0476ae208f21bc63956f748:moodie00
25f9e794323b453885f5181f1b624d0b:123456789

Hashing Algorithm used is MD5

Level of protection:

MD5 (message digest algorithm) is a bad password hashing algorithm because it is too fast and memory conserving so the attacker compute the hash of large number of passwords in very less time.

Recommendations to implement password:

- Try using better algorithm in place of MD5. Eg.SHA256, SHA512
- Always use salts with hashes where feasible.
- for better security use slow algorithm like bcrypt. Which make harder for attacker because it requires more CPU cycles to authenticate user.

Observations on organization password policy:

- weak hash functions used with no salting
- common passwords are used which can be easily guessed and cracked
- No use of capital letters, numbers and special symbols together.

Changes to be made in password policy:

- we can increase the password length to 12 because less characters length it becomes easy for hacker to crack the password using brute force attack.
- Don’t use common phrase as password. Use of mix characters.
- check your password security with password strength checker tools and websites.