Dear Sir/Ma’am

I discovered several weaknesses in your password policy while trying to decipher all the leaked hashes, and this email summarizes my findings and offers recommendations for how to strengthen your password policy.

**Findings**

All the passwords were encrypted using weaker hash algorithm – **MD5**. MD5 is insecure and provides a **very low level of protection** and should not be used in any application. With the help of crackstation.net, it was very simple to crack.

**Organization’s password policy**

1. Minimum length for password: 6.
2. No specific rules/ conditions for password creation (i.e., users are free to use any combination of word and letters to create a password).

**Possible controls to be implemented to make cracking much harder for the hacker in the event of a password database leaking again**

1. Passwords should have a minimum length that is neither too short nor too long.
2. Inclusion of special character, Capital and Small letters, numbers in password.
3. Using high-level protection algorithm (example: SHA-256 or SHA-3) instead of MD5.
4. Use salting to avoid the usage of rainbow tables which accelerates cracking.

**Possible changes in Password policy to make breaking the passwords harder**

1. Minimum length for password: 8.
2. Minimum one special character, one numerical and one character to be used in password.
3. Users shouldn't be permitted to create passwords using their username, real name, date of birth, or other personal information.
4. Passwords must not contain common words and character combinations.
5. The strength of the password should be displayed to the user as they type it in using an external API-based.
6. A software that makes recommendations for enhancing the strength of password.

Thanking you,

Name: Chebrolu Tejaswi

M.Tech (Integrated) CSE with Spl in Data Science

Vellore Institute of Technology

**HASH CODE HASH ALGORITHM PASSWORD**

e10adc3949ba59abbe56e057f20f883e md5 123456

25f9e794323b453885f5181f1b624d0b md5 123456789

d8578edf8458ce06fbc5bb76a58c5ca4 md5 qwerty

5f4dcc3b5aa765d61d8327deb882cf99 md5 password

96e79218965eb72c92a549dd5a330112 md5 111111

25d55ad283aa400af464c76d713c07ad md5 12345678

e99a18c428cb38d5f260853678922e03 md5 abc123

fcea920f7412b5da7be0cf42b8c93759 md5 1234567

7c6a180b36896a0a8c02787eeafb0e4c md5 password1

6c569aabbf7775ef8fc570e228c16b98 md5 password!

3f230640b78d7e71ac5514e57935eb69 md5 qazxsw

917eb5e9d6d6bca820922a0c6f7cc28b md5 Pa$$word1

f6a0cb102c62879d397b12b62c092c06 md5 bluered

9b3b269ad0a208090309f091b3aba9db md5 Flamesbria2001

16ced47d3fc931483e24933665cded6d md5 Oranolio1994

1f5c5683982d7c3814d4d9e6d749b21e md5 Spuffyffet12

8d763385e0476ae208f21bc63956f748 md5 moodie00

defebde7b6ab6f24d5824682a16c3ae4 md5 nAbox!1

bdda5f03128bcbdfa78d8934529048cf md5 Banda11s