Dear Sir/Ma’am

This email summarizes all findings and suggestions for the improvement of the password policy.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are standard Cryptographic hash functions to provide data security for authentication.

**All compromised passwords were using a weak MD5 hashing algorithm which is prone to collision.**

I used websites like crackstation.com and hashes.com to crack and identify the hash functions provided to me.

**I would suggest to use a strong password encryption method to create SHA-based password hashes.**

After cracking the passwords, we discover the following information about the organization’s password policy:

* Users can use any combination of alphabets, numbers and characters to create a password.
* Minimum password length was 6.

You can include the following recommendations:

* Avoid common words and character combinations in your password.
* Use long keywords, minimum 8 letters should be there.
* Do not reuse your passwords.
* Should have special characters, uppercase and lowercase letters, and numbers in the password.
* Users should refrain from using their username, real name, date of birth and some personal information while creating a password.

**Password and Hashing Algorithm Used:-**

experthead:e10adc3949ba59abbe56e057f20f883e- **123456 , MD5**

interestec:25f9e794323b453885f5181f1b624d0b-**123456789 , MD5**

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4- **qwerty , MD5**

reallychel:5f4dcc3b5aa765d61d8327deb882cf99-**password , MD5**

simmson56:96e79218965eb72c92a549dd5a330112-**111111 , MD5**

bookma:25d55ad283aa400af464c76d713c07ad-**12345678 , MD5**

popularkiya7:e99a18c428cb38d5f260853678922e03- **abc123 , MD5**

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759- **1234567 , MD5**

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c-**password1 , MD5**

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98-**password! , MD5**

liveltekah:3f230640b78d7e71ac5514e57935eb69-**qazxsw , MD5**

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b-**Pa$$word1 , MD5**

johnwick007:f6a0cb102c62879d397b12b62c092c06-**bluered , MD5**

flamesbria2001:9b3b269ad0a208090309f091b3aba9db- **, MD5**

oranolio:16ced47d3fc931483e24933665cded6d- **, MD5**

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e- **, MD5**

moodie:8d763385e0476ae208f21bc63956f748-**moodie00 , MD5**

nabox:defebde7b6ab6f24d5824682a16c3ae4- **, MD5**

bandalls:bdda5f03128bcbdfa78d8934529048cf- **, MD5**

**Thanking you,**

**Name: Madhur Sharma**

**B.Tech in Mathematics and Computing**