I've tried to crack the hashes provided in the password dump file and in this memo, I have mentioned the vulnerabilities in your password policy and also all the findings and suggestions to improve the policy.

**What type of hashing algorithm was used to protect passwords?**

The passwords provided in the password dump file use the MD5 algorithm.

**What level of protection does the mechanism offer for passwords?**

One of its vulnerabilities is that it is considered cryptographically broken as it generates identical hashes for similar passwords. Using tools like Hashcat.com and various other online password cracking tools, it was very easy to crack the passwords.

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

For better security, I would suggest that you use a modern and a strong password encryption algorithms like PBKDF2, Bcrypt, or one that is based on SHA.

**What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?**

Based on the cracked passwords, it was found that the organization's password policy has the required length of a password to be at least 6, and there is no specific requirement for password creation.

**What would you change in the password policy to make breaking the passwords harder?**

The password policy can be improved in many ways. My suggestions are:

* Set the minimum password length to at least 8 or 9 characters.
* Make it mandatory for users to include special characters, numbers, and both capital and small letters in their passwords.
* Prevent users from using their personal details like their name or username in their passwords.
* Avoid common character combinations and words in passwords.

The following findings made from the password dump provided are mentioned below:

**Security Algorithms used:**

experthead:e10adc3949ba59abbe56e057f20f883e – MD5

interestec:25f9e794323b453885f5181f1b624d0b – MD5

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5

simmson56:96e79218965eb72c92a549dd5a330112 – MD5

bookma:25d55ad283aa400af464c76d713c07ad – MD5

popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5

liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5

johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5

flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5

oranolio:16ced47d3fc931483e24933665cded6d - MD5

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5

moodie:8d763385e0476ae208f21bc63956f748 - MD5

nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5

bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5

**Cracked Passwords:**

experthead:e10adc3949ba59abbe56e057f20f883e - 123456

interestec:25f9e794323b453885f5181f1b624d0b - 123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password

simmson56:96e79218965eb72c92a549dd5a330112 - 111111

bookma:25d55ad283aa400af464c76d713c07ad - 12345678

popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered