Subject: Password Policy Review - Findings and Proposed Uplifts

Dear Sir/Madam,
I hope this email finds you well. I recently conducted a review of our organisation's password policy and would like to share my findings and proposed uplifts to enhance our password security measures.

I was able to crack the passwords provided in the 'password dump' file below using crackstation

Source: https://crackstation.net/

Hash	Type	Result
e10adc3949ba59abbe56e057f20f883e	md5	123456

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

experthead:e10adc3949ba59abbe56e057f20f883e - md5 - 123456

interestec:25f9e794323b453885f5181f1b624d0b - md5 - 123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - md5 - qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - md5 - password

simmson56:96e79218965eb72c92a549dd5a330112. - md5 - 111111

bookma:25d55ad283aa400af464c76d713c07ad. - md5 - 12345678

popularkiya7:e99a18c428cb38d5f260853678922e03. - md5 - abc 123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - md5 - 1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c. - md5 - password1

edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 - md5 - password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 - md5 - qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - md5 - Pa$$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06. - md5 - bluered

flamesbria2001:9b3b269ad0a208090309f091b3aba9db - md5

oranolio:16ced47d3fc931483e24933665cded6d - md5

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - md5

moodie:8d763385e0476ae208f21bc63956f748 - md5

nabox:defebde7b6ab6f24d5824682a16c3ae4 - md5

bandalls:bdda5f03128bcbdfa78d8934529048cf - md5

I was easily able to crack the first 13 passwords using crackstation.net

Md5 is the type of hashing algorithm used to protect the passwords.

Md5, the mechanism used for password hashing, **offers a very low level of protection for passwords**. It is important to note that MD5 is now considered to be insecure and has significant vulnerabilities. These vulnerabilities make it easy for attackers to crack hashed passwords using various techniques, such as brute force attacks, dictionary attacks, or the use of precomputed rainbow tables.
One of the main weaknesses of MD5 is its susceptibility to collision attacks, where different inputs can produce the same hash value. This means that an attacker could potentially find different passwords that result in the same MD5 hash, making it easier to reverse-engineer the original password.

To make cracking much harder for hackers in the event of a password database leak, several controls can be implemented:

1. **Strong Password Hashing:** Use a strong and slow hashing algorithm specifically designed for password storage, such as bcrypt, PBKDF2, or Argon2. These algorithms incorporate techniques like salting and key stretching to significantly slow down the hashing process, making it more time-consuming and resource-intensive for attackers to crack passwords.
2. **Salted Passwords:** Implement password salting, which involves adding a random and unique value (salt) to each password before hashing. Salting prevents attackers from using precomputed rainbow tables or other precomputed attacks, as they would need to compute new tables for each salt value.
3. **Increase Password Complexity:** Enforce password complexity requirements. Require passwords to have a minimum length and include a combination of uppercase and lowercase letters, numbers, and special characters. This increases the complexity and search space, making it harder for attackers to guess or crack passwords.

4. **Two-Factor Authentication (2FA):** Implement 2FA as an additional layer of security. This requires users to provide a second form of verification, such as a temporary code sent to their mobile device, along with their password. Even if passwords are compromised, the additional factor adds an extra barrier for attackers.
5. **Regular Password Updates:** Encourage users to change their passwords periodically. This minimises the impact of a password leak and reduces the window of opportunity for attackers to crack passwords.
6. **Account Lockouts and Rate Limiting:** Implement mechanisms to detect and prevent brute force attacks. This can include temporarily locking accounts after a certain number of failed login attempts or implementing rate limiting to restrict the number of login attempts within a specific time frame.
7. **Education and User Awareness:** Promote user education and awareness about password security. Train users on creating strong and unique passwords, avoiding common password pitfalls, and the importance of keeping passwords confidential.

By implementing these controls, organisations can significantly enhance the security of their password systems and mitigate the risks associated with password database leaks.

Based on the information provided, **the organisation's password policy appears to have some weaknesses and room for improvement.** Here are the observations regarding the password policy:

1. **Password length:** The password policy does not specify a minimum length requirement for passwords. This lack of a minimum length makes it easier for hackers to crack passwords, as shorter passwords are generally more susceptible to brute force and dictionary attacks.
2. **Special characters:** The password policy does not mandate the use of special characters. Special characters such as symbols and punctuation marks increase the complexity of passwords and make them more resistant to cracking attempts.
3. **Key space:** The key space refers to the number of possible combinations for a password. Without a minimum length requirement and without specifying the inclusion of special characters, the key space for passwords in the organisation's policy is limited. This decreases the overall strength of the passwords and increases the chances of successful cracking attempts.
4. **Lack of complexity requirements:** The password policy does not mention any requirements for complexity, such as including a mix of uppercase and lowercase letters, numbers, or special characters. Password complexity rules help create stronger and more secure passwords.

Overall, the organisation's password policy seems to be lacking in terms of password length, complexity requirements, and key space.
To improve the policy and enhance password security, it is recommended to implement the following changes:

1. **Minimum password length:** Set a minimum password length requirement, such as 8 characters, to ensure passwords are not too short and easier to crack.
2. **Password complexity:** Enforce the use of a combination of uppercase and lowercase letters, numbers, and special characters in passwords. This increases the complexity and makes passwords harder to guess or crack.
3. **Regular password updates:** Encourage users to change their passwords periodically, such as every three to six months, to mitigate the impact of compromised passwords.
4. **User awareness and training:** Educate users about the importance of strong passwords, the risks of using weak or easily guessable passwords, and provide guidelines for creating and managing secure passwords.

By implementing these improvements, the organization can enhance its password policy, increase the strength of passwords, and improve overall security posture.