MEMORANDUM

To: Concerned Authorities, XYZ Organisation
From: Induja Shankar, Governance Analyst
Date: 24-06-2021
Subject: Assessment of Leaked Passwords

The following are the results of my assessment and analysis of the levels of protection of your respected organisation's IT system. On inspection and testing of the leaked passwords, these are my findings and insights:

- **68.42%** of all passwords were **cracked** successfully.
- **ALL of the cracked passwords** belong to the widely available wordlist RockYou.
- **69.23%** of cracked passwords were **less than 8 characters long.**
  The remaining were still **some variation of 'password'.**
- **Only 15.3%** of the cracked passwords had special characters.
- ALL passwords, cracked and uncracked alike, were **all commonly used combinations of words and numbers.**
- Hashes were **not salted.**

Hashing Algorithm Used: MD5
Level of Protection offered: MD5 is a fast algorithm. Although, it does not prove to be a strong hashing algorithm for that very reason, besides the fact that it is cryptographically weak. Its speed allows attackers to try billions of passwords within seconds using a recent GPU. Rainbow tables now make it even faster to crack MD5 hashed passwords. Hence, security of the passwords is compromised.

Recommendations to Implement Controls:
- Switch to a better, tested hashing algorithm - eg. SHA256.
- Avoid using hash functions directly. Assemble several of them together to form a protocol for an increased level of protection.
- Always use salts wherever feasible.
- Use larger systems of hashing functions designed for hashing passwords like *bcrypt* or *PBKDF2*.

Observations on Organisation's Password Policy:
- Weak Hash Function, no salting
- No rules on password length, capitalisations, using special characters.
- No system to prevent user from using common phrases
- Technologically lagging behind in security

Changes to be made in Password Policy:
- Bring in a system that ensures a strong password is set during creation.
- Updated algorithms and protocols needed.