Dear Sir/Ma’am,

I was able to crack most of the leaked hashes using crackstation.net and hashcat.com and have found several vulnerabilities in your password policy. Below are some of the observations and suggestions I recommend for your organization.

MD5 or Message-digest algorithm was used for data security, which is a weaker hash algorithm and provides a very low level of protection. To make password cracking much harder for the hacker, I would suggest that you should use a high-level hashing algorithm such as SHA which is a modified version of MD5 and provide a high level of protection.

The following are the cons of the organization's password policy:

* Minimum password length is set to 6.
* Users can use any combination of words and letters and the use of special characters is not mandatory.

My recommendations that must be included in the password policy are as follows:

* Avoid passwords that include the user’s name and common words.
* The minimum password length must be set to 8.
* Special characters, Uppercase, and numbers must be included in your password.
* Password strength checker tool should be used to let the user know how weak or strong their passwords are.