Dear Sir/Ma’am

I tried to crack all the passwords given to me using CrackStation.net. CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes.

It turns out that it was extremely easy to crack all the passwords. The estimated time taken to track each password by the computer was around a few nonillion years. I found several vulnerabilities in your system.

Secure Hash Function(SHA) and Message Digest(MDs) are very basic cryptographic hash function to provide data security for authentication.   
All of your passwords used MD5 which is weaker and more prone to collisions.

Based on my research, I found the following-  
1. There is no specific format that is set for your passwords. Users can use any number of letters and digits etc.  
2. Minimum password length is 6.  
3. The passwords are super easy to crack.

You need to use a stronger password mechanism to create hashes for the passwords based on SHA.

My recommendations for your new policy are as follows-  
**1. Use Complex Passwords  
2. Set a greater Minimum Password Length like 8  
3. Utilize Passphrases  
4. Have mandatory Password Resets periods  
5. Restrict Password Reuse  
6. Set Minimum and Maximum Password Age Limits**