Dear Sir/Ma'am,

After trying to crack all the leaked hashes, I found several vulnerabilities in your password policy and this email concludes all the findings and suggestions to improve your password policy.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication. All the password which are compromised were using MD5 which is a weaker hash algorithm and is prone to collisions.

It was very easy to crack with hashcat.com, crackstation.com and rockyou.txt wordlist via terminal and two web browsers. I would suggest that you use a very strong password encryption mechanism to create hashes for the password based on SHA.

After cracking the passwords, we find the following things about organisation's password policy:

- Minimum length for password is set to 6.
- There is no specific requirement for the password creation. Users can use any combination of word and letters to create a password.

You can include several new things in your password policy. My recommendations are:

- Avoid common words and character combinations in your password.
- Longer passwords are better, 8 characters is a starting point.
- Don't reuse your passwords.
- Include special character, Capital and Small letters, numbers in your password.
- Don't let users include their username, actual name, date of birth and other personal information while creating a password.
- Train your users to follow these policies to keep their passwords safe.

Thanking you,
Name: Sumanta Sethi
B.Tech Computer Science & Engineering