Respected Sir/Ma'am

My name is Suraj Kumar Singh , and I would like to bring to your notice my findings in relation to controls used by the organization and I would like to propose some upliftments regarding the same for the vulnerabilities found in our password policy.
Among the well know and historical Hash functions like :
MD4(128), MD5(128) , SHA-1(160) ,SHA-2 (224, 256), SHA-3 (224, 256, 384, 512) which provide data security for authentication .
However , MD4, MD5, SHA1 Are not recommended for usage anymore.

All the passwords which are compromised were using **MD5 Message-Digest Algorithm** which is a weaker hash algorithm and is prone to collisions and suffer from extensive vulnerabilities
Using the resources and softwares available like Hashcat , md5decrypt.net , it wasn't much challenging to crack the passwords.
I observed that the organization's password policy (e.g. password length, key space, etc.) was very weak and not standardized. I would suggest that we use a robust password encryption mechanism in creating hashes for the password based on SHA Hash Function.

I tried to observe and find a pattern in the passwords being used in the organization which are :
• Least Size of the password was 6 which is lesser than the normal password size being used by different online platforms(i.e. 8) and not to mention , length plays a major role in this.
• There isn't any standard protocol or criteria in passwords being set .
• There were too many common passwords being used which are easy to guess as well and don't require any software.

I would suggest the drafting of a password policy which is robust and also has a window for amendments so that we can keep bringing more rules and regulations in setting passwords in the future.
• Passwords which are easy to guess and are common words like abc123 , 123456 etc should immediately be put into a block list of words which can not be used .
• Longer passwords are better, 8 characters is a starting point.
• Ther User IDs should not be used as the password.
• Inclusion of special characters, Capital and Small letters, numbers in your password be mandatory
• Don't let users include their username, actual name, date of birth and other personal information while creating a password.
• All passwords be treated as sensitive, confidential information
• Awareness is spread among the users of the different tools being used and how passwords are being cracked so easily so that there is transparency and the users themselves be careful.

Thanking you,
Suraj Kumar Singh
Bachelor of Technology(2017-2021)
University of Petroleum & Energy Studies ,Dehradun