Dear **company**,

My team and I are more than happy to share some tips on password policy to ensure that your company is able to implement secure passwords and keep everyone safe. I have listed a few tips and hope that this will be of help to **company**!

If you have any questions, please do not hesitate to contact my team as we are happy to help.

Sincerely,

**TeamXX**

**Password Policy:**

**Creating Passwords**

|  |  |
| --- | --- |
| Consisting of: | Avoid: |
| ● Password length of at least 8 characters or more  ▪ Make sure password includes:  ▪ Uppercase letters (A-Z)  ▪ Lowercase (a-z)  ▪ Numbers (0-9)  ▪ Special symbols such as !@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./ | ● Generic Passwords such as “password123” “qwerty” “password”  ● Passwords containing a derivative of username  ● Passwords that have been previously or are in current use with other accounts  ● Using phrases that are easy to guess  ▪ Examples include, names of family members, pets, friends, movies, celebrities, public information that could be known to others  ▪ Personal information such as birthdays, birthplace, phone numbers that others may know  ● Alterations in passwords that are used in other accounts  ▪ Ex. Ilo0veD0gs2345!!2020 →  Ilo0veD0gs2345!!2021 |

**Maintaining secure passwords**

* Do not reuse the same passwords across different accounts
  + Ex. a password used for email logins should not be used to create other accounts
* Change passwords once every 90 days
* Do not share passwords with others regardless of the occasion
* Do not store passwords in places easily accessible to others
  + If they are stored on devices, make sure passwords are encrypted and stored in secure files

**Source:**

https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf