To all employees of XYZ corporation,

It is in the interests of everyone to make sure that passwords are secure and non-trivial; Security is everyone's responsibility. To that end, the IT team has created this guideline for secure passwords:

1. Make sure that your passwords are not written down and openly available on your desks. Do not put your password on a post-it note and put it under your keyboard.
2. Make sure that your passwords are not trivial. Do not create a password that contains dictionary words; 'IHateMyJob1234!' is not a secure password, and will not be allowed. Minimum length, Key space and complexity requirements will be implemented.
3. Do not reuse your previous passwords. The IT team will require that the passwords you use will be reset quarterly, and will remember your previous two years' worth of passwords.
4. Do not reuse passwords from non-work-related sources; if your password from your Gmail account is the same as your work VPN account and your Gmail account is compromised, you have potentially also compromised your work account.

If you are having difficulties with generating the required complexity of the password, there are multiple tools that are available to you. Password generators that are publicly available online can give you the needed passwords, and there are free password manager programs that can help you keep track of these.

If you have any questions or concerns, please reach out to the IT team about the password policy.

Regards,

Group 1 Information Team.