



# Password Policy Guide

In today's world, cybersecurity is becoming increasingly important, it's crucial to keep our sensitive information secure. One of the most important ways to do this is by creating strong passwords and following best practices for password security.

## Password Security Best Practices

- Password must be a minimum of 12 characters (more is better)
- Length trumps complexity (but complexity helps)
- Make passwords easy to remember but hard to guess.
- Do not use passwords based on easily discoverable information like the name of your favorite pet
- Do not use previous passwords or similar to previous passwords
- Every password you have should be unique

## Strong passwords

There are lots of ways to create a strong password which is easy to remember.

### Using a passphrase

- 6MonkeysReating!
- 2Dolphinsswimming?
- Weekendsarefab?

### Use a specific combination (colour - animal - number)

- Blueelephant1635!
- Purpledog9283!
- Greenmonkey248?

### Three random words (what are you looking at when changing your password?)

- Slippercurtaincoffee?
- Laptopmonitorprinter!
- Drinkwindowhorse?

### You could also use song lyrics to make a passphrase or use the first letter of each word as in the example below.

The **s**ilicone **c**hip inside **h**er **h**ead **g**ot **s**witched to **o**verload, **a**nd **n**o **o**ne's **g**onna **g**o to **s**chool **t**oday, **s**he's **g**onna **m**ake **t**hem **s**tay **a**t **h**ome.

**TscihgstoAnoggtstsgmtsah!** = easy to remember but hard to crack!

## Weak passwords

The following is a list of most common passwords which are still being used today by many people.

- Admin
- Qwertyuiop
- 123456
- Password
- Password123
- Abc123
- 654321
- 11111111
- Welcome
- Letmein
- Password1
- Qwerty123
- 1234567890
- 987654321

### Do not use a word that can be found in a dictionary or the name of a person, character, product, or organisation.

- 'Companyname'
- 'Yourname / familymember'

**If you are using anything like the above, you really should change it to something more secure. You are putting yourself and your company at risk!**