Password strength is very important. Please read carefully.

Weak passwords are the easiest way for a hacker to compromise a system. Do not use small or easy to remember passwords.

This includes passwords below 12 characters, that are either all letters or numbers i.e. 1234 or ABCD, or identical passwords for all phone extensions.

Hybrid Comms have secure systems setup to detect fraudulent registrations to our gateways and secure passwords are used on the systems that we supply. However we cannot be held responsible for equipment or security that is managed beyond our network. Please take care not to invite hackers to your equipment with poor security policies.

We will not be held responsible for fraud occurring due to customers maintaining inappropriate password standards. Please make your password secure or you may risk losing money.

We strongly advise all of our customers to adhere to the following guidelines;

1. Most importantly, Phone handset or Softphone device passwords must be secure. Please do not leave your password as the default, please do not set your password as something generic. It is surprising how many systems we check that have '1234' OR 'password' set by the IT department.
2. Keep passwords strong and never share admin access details to Hybrid Flow as anyone with these details can place calls on your behalf. Have a staff security policy in place and always shut down any access when a staff member moves on.

Hybrid Comms Password Guidelines

Hybrid Comms has a set of password guidelines (detailed below) that will result in industry standard secure passwords. We strongly advise customers to follow these guidelines, we will provide assistance where required.

Modifying the passwords for your PBX/Gateway extensions

The passwords should have the following minimum values:

- 12 characters long.
- uppercase letters such as A, B, C;
- lowercase letters such as a, b, c;
- numerals such as 1, 2, 3;
- special characters such as $, ?, &;

With PBX/VoIP Gateway systems, the password changes should be enforced on all extensions (whether they are in use or not).

Once the passwords have been modified following our guidelines below, there will be a significantly reduced risk of your passwords being broken.

How do I change my passwords?

There are plenty of websites out there now that will allow you to easily generate a password from your web browser. It's probably best to use one provided by a security company, such as

https://my.norton.com/extspa/passwordmanager?path=pwd-gen

You can NB. In some cases, passwords containing punctuation cannot be used. If you have difficulties in setting these new passwords on your phone, run the utility again, but omit the punctuation check box.

Please use a password strength meter, such as https://www.passwordmonster.com to check the suitability of your password.