TGC Computers Ltd - Web Access Password Policy

Password Requirements

Customers should be aware that strong passwords are required for all systems and user-access and that a **strict non-disclosure protocol** applies to passwords. Where applicable to the system or device being used, TGC utilises software to enforce the use of strong passwords. You should not share or disclose any password.

Strong passwords are enforced on systems and by users and must be: -

- More than 8 characters in length
- Include letters, numbers and at least 1 special characters
- Cannot use repeat characters (e.g. aaa64135, 111bcxjk)
- Not be easily recognisable *(i.e. no names, dates of birth, places etc*)
- Must include upper and lowercase letters
- Cannot match your Log-In ID (e-mail address)

Tips for Stronger Passwords

- Do not use a word found in the dictionary
- Use a mixture of letters, numbers, and special characters (e.g. h37@f3-2)
- Use a combination of uppercase and lowercase letters
- Use supported special characters (e.g. !, @, #, $, &)
- For a strong and easy to remember password, create a personal acronym
- Use a different password than your other online accounts

All passwords are changed 3 monthly, and users are not permitted to reuse the same password within a 9-month period. This is forced policy using software on all systems and a password change is automatically promoted at the start of each month. This change is enforced within 5 days of the change reminder being shown.

If a user fails to use the correct username and/or password when logging in to a system or device, we utilise generic failure messages that do not disclose the exact nature of the login error. After 3 failed attempts, the system will advise that login has failed, however it will not disclose if this is due to the username, password or both being incorrect. This aids in preventing brute force attacks or a non-authorised user being aware of which field is incorrect, which then increases their login attempts.

Where login fails, we operate a three-strike approach and the system will become unavailable for 15 minutes before the login can be re-tried. This protects against external ‘bot’ attacks and brute force.