



## Client Zone Data Protection

---

All client zone data is stored in a MySQL database which is password protected and is only accessible via the client zone interface.

All users accessing the client zone have to logon with a user name and password.

User names are set up by P Hull Only, users cannot create accounts online.

User passwords are set and issued by P Hull, assuring that strong passwords are used for all client zone logins.

Brute force protection built in, to protect against brute force attacks on the client login. Effectively restricting the number of invalid user logins per minute, requiring the user to wait 10 minutes before being allowed to attempt to login again.

Coded with “prepared statements” to protect against SQL injection attacks.

Server side firewall to protect against server side attacks, including:

A Stateful Packet Inspection (SPI) firewall, Login/Intrusion Detection and Security application for Linux servers. IDS (Intrusion Detection System), SYN Flood protection, Ping of death protection, Port Scan tracking and blocking, Permanent and Temporary (with TTL) IP blocking, Exploit checks.

## Data Backup

---

We are currently using a web hosting account on our private cloud infrastructure from CWCS Managed Hosting to host the client zone. This private cloud is housed in one of their UK datacentres.

The web hosting account is backed up daily to a remote backup server within CWCS’s datacentre.

The hosting account (for both the website and client zone) is also backed up nightly and sent via secure FTP to an off site server outside of the CWCS’s datacentre. This copy is then backed up twice to additional NAS drives.

A facility is also provided within the client zone administrator area to make a local back up of the MySQL database whenever required. It is good practice to use this facility at the end of every day.

Document last updated: 11/10/2018 15:42:00