DECORUS for sage

Cloud Server Security and Backup Policy

Our goal as a server provider is to deliver a stable fast platform safe from internal and external threats for customers to use their software. For this to happen there are a number of things that we have put in place. Unfortunately, by ourselves we cannot guarantee the security of customers' cloud server. It is also up to the users to make sure that they keep their login details safe and away from unauthorised users and make sure that they log off the server when they are away from their desks.

Security and Data Backup Measures

Below is a list of the security and data backup measures put in place to ensure the safety of customers' servers:

- **Dual layer configured firewall** – This will protect the server against intrusions and malware/viruses

- **Encrypted remote connection protocol to the server** – Microsoft Remote Desktop Connection is encrypted meaning that transferring files to and from the server is secure.

- **Shadow backups** – Shadow backups are taken every 6 hours to protect from data loss and accidently deleted files.

- **Full System backups** – backups of the entire server are taken daily to ensure that the server can be quickly restored back to a working point in the event of any system failure.

- **Offsite Backups** – Server data is also backed up to a second site daily and with monthly backups being saved for a full 12 months.

- **Full System Rollover** – All of our cloud servers are configured with system rollover to prevent server downtime. Rollover works by transferring servers over to new hardware automatically in the event of any failures. This is done automatically and without any downtime for the user.

- **Configured Desktop Environment** – The desktop environment on the servers that users will be accessing has been configured to minimise the damage caused by user error or unauthorised users.

- **Secured Web Browsers** - The web browsers used on the servers have been configured to prevent harmful files from being downloaded.

Effective use

For the measures put in place to be at their most effective users must take note of the following:

- User login details must be kept secure and out of the hands of unauthorised users;
- Users must not try to install additional applications on the server;
- Users must not copy any potentially harmful files or packages onto the server;
- Users must not make any changes to the configured desktop or web browsers;
- Whilst the server has several backup options to restore your data we stress that the Decorus and Sage data on the server is still the responsibility of the customer and taking backups within the software is highly recommended. This way customers are able to restore data to fix accidental errors independently without the assistance of our technicians.

Provided users follow the guidance above you will find your cloud server to be effective and secure.