
FAQ's

Q. What backup technology do you use?

A. Redstor online backup is powered by Attix5's Backup Professional software. Redstor online backup is secure, reliable, online and fully scalable.

Q. What port is used to transmit information to the backup site/server?

A. All communication between the backup client and Redstor's storage platform is sent via port 443.

Q. What encryption technology is used to encrypt data being transmitted over the internet?

A. 256 AES & SSL 448 Blowfish encryption.

Q. How fast are your data-centre connections to the internet?

A. We have 200MB's download and 200MB's upload from and to our data centres. 'On-Net' and VPLS connections available.

Q. What encryption technology is used to store backed up data?

A. 128 bit AES & SSL 448 Blowfish encryption.

Q. What happens to our data when we leave?

A. The account will be available for recovery of data for the period of time agreed in your SLA, after which the account is deleted and access to your stored data is lost. All archived data stored on any off-site tapes will remain in its encrypted form, unreadable and useless. If this is not satisfactory you can request for archived data to be totally deleted but this is chargeable work due to its labour intensive nature.

Q. What disaster recovery and business continuity measures does Redstor have in place?

A. Redstor offers a comprehensive DR infrastructure. We have two data centres linked by a high speed fibre network. All of our data is replicated between these two sites

over a SSL encrypted line. We have a fully resilient configuration and can switch across to the DR site with minimal impact to our clients.

Our primary data centre is:

- Manned 24x7
- Accredited to Quality standard ISO9001:2000*
- *which includes:
- BS7499 - Manned Guarding & Mobile Patrol
- BS7984 – Key Holding
- BS7858 - Vetting
- BS7958 - CCTV Public Space Surveillance

Q. Are Virtual platforms supported?

A. Yes. Virtual environments are supported. For example, VMware vSphere servers.

Q. Does the backup software have an audit trail?

A. Yes Redstor Online Backup does create an audit trail.

Q. Can you have different levels of backup/restore rights e.g. Finance users cannot see HR.

A. It depends. You can adjust the service permissions so that the backup client has the access rights of the user credentials entered but you cannot set individual user rights to the backup client.

Q. Are open files backed up?

A. Yes. Open files are backed up. The application uses VSS (volume shadow copy service) to backup any file currently in use.

Q. Is there a version of the backup stored on a local server onsite or is it possible to have this in place?

A. Yes. You can choose to cache a local copy of the data. You can also select how many days worth of backups are stored locally with the only limitation being local disk space.

Q. Do you charge for full restores (DR tests) carried out bi-annually?

A. Data is always available for restore over the internet, free of charge, including for disaster recoveries.
In the event that data cannot be restored over the internet in an acceptable time frame, data can be provided for restore using portable media, for example a USB or

portable NAS box. In the event that this is required, Redstor can either bring the device containing the data to site to assist with the recovery or the device can be couriered to the required location – both of these options are chargeable, per incident.

Q. During a DR scenario can you prioritise which data, files or servers are recovered first?

A. Yes, however, you must do so manually. There is no automatic feature within the backup client that will allow the functionality.

Q. In a DR scenario how do you handle recoveries? e.g. Online, tapes or HDD

A. It depends. We can send the restore data to you via the internet or you can arrange to have the data sent to you on disk. If archived data resides on tape then we can have the data transferred to disk and then delivered to you. The service is designed to be as flexible as possible.

Q. Can data be restored to a different site if required?

A. Yes, data can be restored to another location provided you have the necessary security information (encryption key and passwords). For smaller restores there is the option of using our web based recovery software which will allow you to access your data from anywhere in the world providing you have internet access.

Q. Are security measures in place to stop someone from restoring data to another site?

A. Each account requires an encryption key and username and password. Without these details you cannot perform a restore of data. You can even add a password to the backup client itself to stop unwanted access to the client.

Q. How many generations of backups can be kept?

A. Data is kept live on the Storage Platform for up to 60 days, and thereafter consolidated into 1 month-end. To give an example, if a backup client begins to backup during January, by the end of February, any specific backup taken during January and February can be recovered. During the first backup in March, all the backups for January are consolidated into a month-end backup.

Q. What process does Redstor have in place to handle a primary data centre failure?

A. Below is the process that Redstor have for in place for a data centre failover:

-
1. As the user attempts to backup, the connection is authenticated with an authentication server which directs the client to an available backup server.
 2. In the event of the authentication server being unreachable the user can authenticate with a secondary authentication server hosted in the secondary data centre, the client holds credentials for both the primary and secondary servers for this purpose.
 3. If the primary site is available, the client will be directed to the Primary Backup Server.
 4. If the primary site is unavailable, the primary or secondary authentication server will direct the client to the Secondary Backup Server.
 5. Data is sent to the correct IP.

Q. Is the remote backup service PCI compliant?

A. PCI compliance is not about a technology or service being PCI compliant, it is all about an organisation itself being PCI compliant - by meeting a broad set of criteria, as outlined in the PCI standard. The standard basically incorporates a set of best practices around security and data privacy. There are 12 requirements that make up the standard:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Your online backup solution will **help** an organisation move towards/achieve PCI compliance as it protects stored data and it encrypts data in transit (and stored in our data centre), satisfying requirements 3 and 4.