Backup and IT Security Policy

This policy applies to the servers utilised by Compressed Air Solutions Ltd. This policy should be read in conjunction with the company's Data Protection Policy and Privacy Policy.

The purpose of this policy is as follows:

- To safeguard the information assets of Compressed Air Solutions Ltd
- To prevent the loss of data in case of accidental deletion or corruption of data, system failure or disaster.
- To permit the timely restoration of information and business processes, should those events indicated above occur.
- To manage and secure back up and restoration processes and the media employed in the process.

Security: Hardware and Software

Hardware (Server and NAS-drive) at Compressed Air Solutions Ltd is held in a secure location on site. The hardware is protected against damage from spikes of electricity from the grid by a UPS (Uninterruptible Power Supply). The UPS is regularly checked by the account administrator and replaced when necessary.

The hardware is held in a secure location and data will be backed up in accordance to the schedule below:

All Data (company files, database) stored on the CAS server will be regularly backed up as follows:

- Full back up daily (Monday-Sunday) – locally via two servers
- Off site back up of company files (excluding emails) occurs Monday-Sunday in the evenings (to the cloud)
- The email system utilises Microsoft 365 exchange.

The software at Compressed Air Solutions Ltd is a Windows Domain Server that controls user access through security policies. There is one administration account that is managed by one nominated Account Administrator, authorised by the company Directors. All data stored is only accessible by those with authorised access and no account has access to folders that have not been permitted by the Directors.

Backup Verification:
Backups will be verified periodically to check for and correct errors, to monitor the duration of the backup and to optimize back up performance where possible.

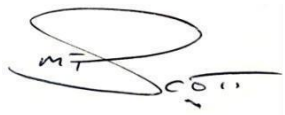
The Account Administrator will undertake random test restores to verify that backups have been successful. These will be completed at least twice a month. Periodic checks may also be undertaken by BSI as part of the ISO: 9001 2015 Quality Management assessment visits. Any problems identified will undergo corrective action to reduce any risks associated with failed backups. Corrective actions will be completed by the Account Administrator.

Data Recovery:
In the event of a catastrophic system failure, off-site backed up data will be made available to users within one - five working days; depending upon the data required and allowing time for destroyed hardware and other equipment to be replaced. Access to the database will be restored within 24 hours by the Account Administrator.

In the event of a non-catastrophic system failure or user error, on-site back up data will be made available to the user within one working day.

In the event of accidental deletion or corruption of information, requests for restoration of information can be made to the Account Administrator.

This policy will be reviewed on an annual basis, unless otherwise required, and disseminated electronically to all employees. A copy will be made available to all interested parties on request.



Mark Scott, Managing Director
17th April 2023