Information 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 Security Measures

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, emails) 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)
- A cloud-based exchange server is used for the storage of emails

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.

The company use a Microsoft Defender programme for anti-virus security; updates/checks are made on a regular basis by the Account Administrator.

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 on a weekly basis. 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.

Internet and Email use:

Email services are provided by the Company primarily for business purposes. Users (employees, agency staff and contractors who have access to email systems) are permitted to use email for reasonable personal use provided there is no adverse impact on Compressed Air Solutions Limited business, costs, employees or relationships with stakeholders. If a conflict occurs between business use and personal use then the business use will take precedence. This policy does not confer a right to use Company email services for personal use.

The following restrictions apply to both business and personal use unless otherwise stated.

No usage may be made of email services that result in any of the following:

- Failure to comply with any terms and conditions of employment;
- Failure to comply with any contract;
- Failure to comply with Compressed Air Solutions Limited security policy, principles and procedures;
- A breach of the law;
- Disclosure of confidential, restricted or personal information without appropriate authority or in contravention of the General Data Protection Regulations;
- Disruption to Compressed Air Solutions Limited services;
- Adverse impact on Compressed Air Solutions Limited business;
- Malfunction of any Compressed Air Solutions Limited equipment or software;
- Corruption or loss of any Compressed Air Solutions Limited data.

No material will be sent or forwarded that is:

- Offensive including pornography, explicit or obscene language or of an inflammatory nature;
- Discriminatory to on the basis of, for example but not restricted to, skin colour, race, religion, age, gender, marital status, disability, carer status, sexual orientation, ethnic or national origin, political beliefs or social position;
- Threatening or harassing;
- Relating to illegal activities;
- Operating a personal business or soliciting money for personal gain;
- Originating or sending chain email or spamming.

The following points are offered as guidelines to help staff manage their email account:

- Remember to check your mailbox regularly;
- Reply to incoming emails as soon as possible;
- Send emails only to those who really need to know;
- Ensure that 'out of office' notification is set when you are away from the office;
- Delete messages that are no longer needed, regularly emptying your 'deleted items' or 'trash' folder;
- Think about whether email is the most appropriate medium for the particular message or information that you have;

- Keep messages brief and check spelling;
- Use precise subject titles;
- Communicate courteously;
- Never include personal details except where absolutely necessary;
- Do not send email to someone who has requested that you do not do so;
- Do not append attachments unless absolutely necessary, especially when these are large files that could impede the network.

The Company reserves the right to monitor employees' e-mails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The Company considers the following to be valid reasons for checking an employee's e-mail:

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.
- If the Company suspects that the employee has been viewing or sending offensive or illegal material, such as material containing discriminatory terminology or nudity (although the Company understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the Company suspects that an employee has been using the e-mail system to send and receive personal communications.
- If the Company suspects that the employee is sending or receiving e-mails that are detrimental to the Company.

The Use of Removeable Computer Media:

The use of storing/transferring data on USB drives is only permitted when the information contained does not contain any personal or sensitive data relating to an employee or any other stakeholder of the business (including customers and suppliers). Examples of permitted data includes data logging information, policies or procedures, company specific certifications.

Reporting IT Security Breaches:

Employees should notify the Directors and the IT Accounts Administrator immediately if they suspect any IT security breaches. The Directors will comply with the GDPR and notify the Information Commissioner within 72 hours if there is a data breach.

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
11th July 2022