DATA PROTECTION & SYSTEM SECURITY

Bravo Benefits take system security seriously.

The purpose of this policy is to outline the steps taken by Bravo Benefits to ensure cyber security.

1. Our internet connection is secured by a Firewall
2. Our devices have the most secure settings
3. Our devices are encrypted and/or password protected
4. Default passwords are never used, they are immediately changed upon set up
5. Staff only have access to what is required for them to perform their role
6. Staff are unable to download software on their devices
7. Anti-malware software is installed across all devices
8. All patching is applied within relevant time frames
9. Devices are regularly checked to ensure they are up to date with system updates
10. Data is stored in the UK in a secure data centre and can only be accessed by approved individuals
11. A secondary back up is kept of all data held within our platform. Off-site back-ups are encrypted and only in the possession of a single individual. De-encryption keys are stored separately
12. All traffic to the Bravo Benefits site is encrypted using HTTPS across modern cryptographic protocols with a Quality SSL A rating
13. Comply with the Payment Card Industry Data Security Standard (PCI DSS) when processing card payments
14. Annual Penetration Tests conducted by a UK based CREST certified team

DATA PROTECTION ACCREDITATION

We are fully registered with the Information Commissioner's Officer (ICO), our registration number is Z2411286.