Mantle Services Security Policy

Security Policy

This document is the Mantle 'Security Policy' in effect from 1 April 2023 and referred to within the agreement between Mantle and their customers. The Policy is available to Customers via the Mantle website and may be varied from time to time by Mantle, reflecting changing business, operational and technological circumstances. All Customers will be notified of the issue of any amended Policy, and can view this on www.mantleservices.com or any other website address as may be notified to the Customer from time to time.

1.	Mantle's hosting provider and affiliate, Mantle Hosting Limited will maintain ISO27001:2013 (Information Security Management System) accreditation and CSA (Cloud Security Alliance) STAR continuous monitoring certification in respect of the Software. Cyber Essentials Plus will also be maintained. All relevant certificates will be made available to customers on request.
2.	Mantle will undergo a third party penetration test annually, using both black box and white box techniques. Reports of such penetration tests, redacted for security reasons if necessary, will be made available to customers on request.
3.	Within Mantle's database all personally identifiable information is encrypted in transit, and at rest. Backups are fully encrypted. Documents uploaded to the database are encrypted. All data encryption will use the AES256 cipher in CBC mode. Encryption keys will not be stored on the same virtual servers as the data they encrypt. Full disk encryption is enabled.
4.	Public Cloud Providers hosting Mantle virtual infrastructure will have no access to encrypted or unencrypted scheme or membership data. No third party providers, with the exception of authorised third party penetration testers granted temporary access, will have access to encrypted or unencrypted Customer Data.
5.	Mantle will maintain a log of all actions by Authorised Users, including read only access to data, and will log times, IP addresses and any other information required to trace access to data. Such access logs will be stored until the data to which they relate has been removed from the system by customers.
6.	Mantle has a process of continuous security review, and ensures that Mantle adopts industry best practice to mitigate any electronic threat to the Services. Full details of the security measures are available on request.
7.	Mantle will include tools that allow GDPR Data Subject Access Requests to be made, and that allow data to be removed entirely for a Data Subject if the customer requires it.