TAKING CONTROL

mantle®

Mantle - Privacy and Security Policy
April 2018

This document is the Mantle "Privacy and Security Policy" operated by Pensions Hosting Company (PHC), with effect from 1 April 2018, and referred to within the Mantle Services Agreement between PHC and their Customers. The Policy is available to Customers via the PHC website and may be varied from time to time by PHC, 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.mantlehosting.co.uk or any other website address as may be notified to the Customer from time to time.

Privacy and Security Policy

1. PHC will maintain ISO27001:2013 (Information Security Management System) accreditation and CSA (Cloud Security Alliance) STAR continuous monitoring certification in respect of Mantle. Cyber Essentials Plus shall also be maintained. All relevant certificates shall be made available to customers on request.

2. Mantle shall 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, shall be made available to customers on request.

3. Within the Mantle database all personally identifiable information is encrypted. Backups are fully encrypted. Documents uploaded to Mantle are encrypted. All data encryption shall use the AES256 cipher in CBC mode. Encryption keys shall not be stored on the same virtual servers as the data they encrypt.

4. Public Cloud Providers hosting Mantle virtual infrastructure shall have no access to encrypted or unencrypted scheme or membership data. No third party providers with the exception of third party penetration testers granted temporary access shall have access to encrypted or unencrypted scheme or membership data.

5. PHC 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 shall be stored until the data to which they relate has been removed from the system by customers.

6. PHC 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.

9. Mantle shall include tools that allow GDPR Data Subject Access Requests to be made, and that allow data to removed entirely for a Data Subject if the customer requires it. Deletion of data shall become permanent only after the standard backup retention period of 90 days.

April 2018