Connect Super Data Security and Privacy

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorised or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all of our and all customer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our staff.

1. Data Transmission

To ensure the security of sensitive information, Connect Super provides clients with a login to a secure portal for the upload and download of required documents. Email is only ever used where the portal is temporarily unavailable and the transfer of data is urgent.

2. Data Storage

The bulk of each fund's information is held within Class. Class' production systems are spread across two hosting providers, Macquarie Telecom (MacTel) and Amazon (AWS), both residing in Australia.
MacTel and AWS certifications and standards ensure that data is only accessible to authorised staff.
Access to the data is only granted on an as required basis and the hosting organisation does not have access to it. Physical access is limited as server racks are located in locked cages.
In some circumstances, Connect Super will require that client documents be transmitted and/or stored using third party document management systems e.g. Dropbox, Onedrive, etc. as this is a more secure and practical bulk file transfer method than email. Where this is necessary, the third party's security and privacy policy is first reviewed to ensure it complies with Connect Super's security standards before the third party service is deployed.

3. Data Control

All data is wholly controlled by Connect Super. If for any reason Connect Super requires other parties to handle data (e.g. contractors and specialists) then appropriate reciprocal arrangements, such as Non-Disclosure Agreements, and adherence to Australian Privacy Principles are put in place to safeguard the data. Access to the data is only granted on an as required basis.

4. Backup and Data Loss Prevention

A replica of the Class production database is maintained at all times on duplicated hardware. An automatic data replication service duplicates the production data on to the alternative "warm standby" system at intervals of no greater than fifteen minutes.
To manage the risk of an entire datacentre failure, in addition to the above, an entire off-site replica of the Class System is maintained on Amazon's Cloud infrastructure which is kept up-to-date using data updates shipped at a maximum interval of 15 minutes.

5. Privacy and Access Control

Privacy is managed via the use of privileges based on individual credentials. These are mapped in a granular fashion to ensure an individual user has access to only the data that they are entitled to view and modify.

6. Maintaining Private Information

Connect Super has adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The NPPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information.

When we collect private information we will, where appropriate and where possible, explain why we are collecting the information and how we plan to use it.

When client data is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify it. However, we are generally required to keep a record of client files for a minimum of 7 years.

Further details of Connect Super's privacy policy can be found at www.connectsuper.com.au