## Data Security for the Docscentre Platform

The Docscentre platform is authorised by the ATO to provide Digital Services, which is regulated by the ATO and the ABRS. The service undergoes annual audits to ensure compliance. In addition, service providers must ensure that data shared via API's also comply with the ATO requirements.

The team at Docscentre ensures that the platform continues to meet its obligations for the benefit of our users and customers to keep their data safe.

The company maintains up to date virus and firewall protection systems, ensures all third-party software are kept up to date and staff are vetted, authorised and trained on the policies for data security and protection.

### Access & Authentication

All user-based access must be controlled by a unique username and password.

- Shared logins are not permitted and must be blocked by Docscentre
- Remember-me functionality must be limited to less than 24 hours
- Multi-factor authentication (MFA) is mandatory and does not include social media logins, for example, Google/Microsoft/Facebook.

### Data Hosting

All data is hosted onshore, including redundant systems, and is managed by Australian owned businesses.

### Encryption Key Management

The company employs Encryption Key Management and Public Key Infrastructure which includes asymmetric/public key algorithms, hashing algorithms and symmetric algorithms as per Australian Government guidelines.

### Encryption at Rest

Data is encrypted at the disk, container, application, or database level. Encryption at rest follows Australian Government guidelines.

### Encryption in Transit

Data is encrypted in transit by an endorsed and approved cryptographic protocol, as per Australian Government guidelines.

Docscentre (ABN 14 096 781 976) is 100% owned by Sequoia Financial Group Ltd ASX:SEQ