your Digital file®
SMARTER SECURITY

The Cryptoloc® Advantage

Who stores and controls the keys to your files?

Document Encryption Keys are generated by the user and protected using patented Cryptoloc® technology. The user is always involved in the encryption and decryption process.

How does this affect the security of your files?

Our Document Encryption Keys are generated by the user, who is always in control of their data.

Other online storage providers generate and store all Document Encryption and Decryption Keys on their servers which, if compromised, directly expose the user's data, making all files accessible by the attacker.

Why is Your Digital File's security superior?

Q Are the documents protected by more than just "username and password"?

Yes

- Every user creates a password-protected digital private key when they sign up to Your Digital File
- The private key is generated and saved on the user's device and is never transmitted to Your Digital File
- The private key is required for all critical actions in Your Digital File — sharing & authorising, signing, nominating and encryption & decryption

Q Does the service provide Advanced Key Management?

Yes

Your Digital File's Document Encryption Keys are never stored in a complete form and cannot be decrypted by any single party alone, including Your Digital File

Q Are the Document Encryption Keys created on the user's computer?

Yes

The Document Encryption Keys are generated by the user, on the user's device

Q Can the Document Encryption Keys be decrypted only by the user?

Yes

The Document Encryption Keys are not able to be decrypted by the service. Decryption always happens on the user's device

How does Your Digital File deliver Advanced Key Management for maximum information security?

Advanced (Document) Key Management is provided by our patented Cryptoloc® technology and is superior to many other cloud services as users' document encryption keys cannot be decrypted by our servers.

- ✓ Your Digital File's Document Encryption Keys are never stored in a complete form and cannot be decrypted by a single party
- ✓ Each Document Encryption Key is made up of three master keys, which are shared between the three parties defined in the system (user/service/escrow), two of which must collaborate to decrypt a document

The Cryptoloc® Advantage

- ✓ Advanced Document Key Management and simplicity of use
- ✓ Integrity and validation of all important user actions (all critical user actions such as sharing & authorising, nominating, signing and all permissions require the User's private key)
- ✓ A Data Legacy service, enabling your data to be accessible to authorised parties in the event you or your business ceases to exist

Where is your data stored?

Your Digital File's servers are based in ***Australia*** where data is governed by ***Australian law***.

Many other cloud services rely on ***third-party*** file storage services, such as ***Amazon S3***, which has servers located in ***America***, ***Europe*** and ***Asia***.

Australian law does not govern or protect data stored in overseas servers.