DAATS

DIGITAL & AUDIO TRANSCRIPTION SERVICES

DAATS PTY LTD SECURITY POLICY

Secure file storage

All clients are to upload their files to our secure server, ShareFile which stores and sends encrypted files. ShareFile's servers are based in Sydney, Australia.

Our privately managed server farm is equipped with the latest firewalls and computer internet security updates to help keep your data completely safe.

All communications between the server and the user are encrypted using the Secure Socket Layer (SSL). This is the same functionality used by banks and popular e-commerce services such as Amazon.com for secure communication. The server also offers the ability to store your files encrypted when they are at rest on our servers, adding an additional layer of security.

When our staff create folders in the system, only the specified users that are designated by owner of the folder are able to access the contents of those folders. Users who do not have access to the folder will not even see the folder in their view of the system.

Each user of the system has a unique login and password. All user passwords are hashed in the server's database, meaning that not even the server's support personnel have the ability to view or in any way determine a user's password.

The server's computer network security is subject to daily security audits by a third-party security monitoring firm. This helps us stay one step ahead of the latest security threats.

The following security procedures are adhered to by all DAATS admin staff and subcontractors.

These procedures enable us to provide the highest security possible and therefore protect your confidential information.

- All new clients are issued a secure login and password to upload their information to DAATS secure server.

- Clients are requested to upload documents or files to their own personal folder via secure login and passwords.

- DAATS admin staff download the files in order to review them and determine the suitable typist for the work.

- All documents or files are then sent via the server to the typist, who downloads the file and imports into the necessary software to complete the job.

- Once the job is complete, the typist uploads the completed document to the server.

- The admin staff then send the completed document and corresponding file/s, via the secure server, to the proofreader (if the job is a transcription job) who downloads the document and proofs the document whilst listening to the audio.

- Once the proofreader has completed the document, they upload the final document to the secure server.

- Our admin staff then download the final document and review the document once more before uploading to the client's completed folder.

- The client is notified via email that the document is completed and can download via a link contained in the email.

- All subcontractors delete any documents and audios from their software; recycle bin and hard drive, within 48 hours of uploading the document to the server.

- All admin staff delete all audio and documents from their software, recycle bin and hard drive within 7 days of upload to the server.

- All documents and files_remain on the server for 30 days unless the client requests a different time.

- All completed documents_remain on the server for 30 days unless the client requests a different timeframe.

- DAATS will only use email for forwarding of documentation by the request of the client.

- All DAATS staff and subcontractors are required to have the latest anti- virus software installed on their computer and update this software when required.

This security policy is signed by all DAATS admin staff and subcontractors.