DAATS
DIGITAL & AUDIO TRANSCRIPTION SERVICES

DAATS PTY LTD PRIVACY POLICY

At DAATS Pty Ltd, we recognize that privacy is extremely important to our clients. This privacy policy has been created to demonstrate how we at DAATS are committed to protecting your confidential information.

We undertake the following measures to ensure a maximum level of privacy is practiced for all our valued clients.

Policy coverage

This policy outlines how DAATS handles the personal information collected by its clients. Your personal information is not distributed publicly and only kept online for administrative purposes.

Use of Personal Information

We do not distribute the personal information of our clients to our typists or proof-readers, they are only given access to the audio files. The only information given to typists is that which is necessary for proper completion of transcripts.

Secure file storage

All clients are to upload their files to our secure server, which stores and sends encrypted files.

Our privately managed server firm 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 creates folders in the system, only the specified users that are designated by the 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.

Uploading of audio files

All clients are given a unique secure login and password and we create a personal folder for you. The client, being the owner of the folder, has the ability to access the contents of those folders and upload audio files to these folders. DAATS administrative staff are automatically notified via email that a file has been uploaded to the server. Our admin staff then download the file from the server and it is allocated for typing.

Completed documents

Once your document is completed, it is uploaded to the client's folder through the secure server and an email notification is sent to alert the client that the document has been completed. We will only email completed documents upon request.

Retention of audio files and documents

All audio files remain on the server for 30 days and they are then permanently deleted from the server.

All documents and audio files are deleted from the typists' computers and hard drives within 48 hours of uploading these to our server.

All documents and audio files are deleted from our admin computers and hard drives within 7 days of uploading these to our server.

All documents and audio files are deleted from our servers within 30 days.

Files will only be retained for longer upon request from the client.

Employee and subcontractors

All employees and subcontractors working for DAATS must also sign a confidentiality agreement prior to undertaking any work.