SpeechWrite 360

360 Data Security

DATASHEET

SpeechWrite 360 is a state-of-the-art dictation and voice recognition workflow solution for the legal sector, allowing authors to record and submit dictations using a variety of methods such as mobile applications and telephony, as well as receiving and managing transcriptions.

Security, reliability, and integrity of both the system itself and the data contained within are taken very seriously by SpeechWrite, and as such we have employed several techniques and industry-standard technologies to achieve those goals.

Hosting and Certification

The SpeechWrite platform is hosted entirely in the cloud on Amazon Web Services. The AWS cloud infrastructure offers the most powerful, flexible and secure cloud-computing environment available today. AWS services comply with the General Data Protection Regulation (GDPR).

AWS has achieved a number of internationally recognized certifications and accreditations. In the process, AWS has demonstrated compliance with third-party assurance frameworks such as ISO 27017 for cloud security, ISO 27018 for cloud privacy, PCI DSS Level 1, and SOC 1, SOC 2, and SOC 3.

Active Directory

The system supports the use of authenticating logins against an Active Directory configuration.

Database Encryption

The SpeechWrite database, logs, backups, and snapshots at rest are encrypted using 256-Bit AES and network-isolated.

Network Communications

HTTPS

All network requests from a client application, be it a web browser or a mobile application, to SpeechWrite's servers are secured by using the HTTPS (secure HTTP) protocol. This mitigates the risk of man in the middle attacks by authenticating the application as belonging to SpeechWrite and not to a malicious third party. HTTPS also provides bidirectional encryption between client and server, preventing eavesdropping or malicious tampering of requests.

IP Locking

The system can be configured to utilise IP locking for accounts, preventing access to that account if the client's IP address does not fall into a predefined range.

User Login

Hashed Passwords

Users access the system through a username and a password. The password is hashed before being stored and is "salted," which concatenates a random value to the password plaintext before being hashed. This means that no plain text passwords are stored anywhere in the system. Passwords can be set to expire and require regular rotation.

Two–factor Authentication

The system supports the use of two-factor authentication, using a combination of password and time-based one-time password (TOTP) security. This requires a user to provide both a valid password and a time-limited authentication code that is generated using a mobile app such as Google Authenticator. This mitigates the risk of a security breach in the event of password compromise.

Delivering efficiencies through voice

0121 236 2626 | 360@speechwrite.com

www.speechwrite.com

SpeechWrite Digital