Interpreter SOC 2 security overview

Overview

Interpreter provides a real-time transcription and translation platform for over-the-phone interpreters. The platform processes spoken audio across 60+ languages and delivers live translations during interpreting sessions. It is available as a web application and a Chrome browser extension.

Interpreter is designed so that audio and transcript data never reach Interpreter's servers. The only data stored is basic account information and session duration for billing.

This document describes the security controls Interpreter has implemented, organized around the SOC 2 Trust Services Criteria for security. Interpreter's speech recognition provider holds a SOC 2 Type II certification with a clean audit opinion.

System description

Services provided — Interpreter captures audio from the user's browser and streams it directly to a speech recognition provider for transcription and translation. Results are displayed in real time. The platform handles user authentication and billing based on session duration. Interpreter does not store audio or transcripts.

System boundaries — The in-scope system includes:

- Interpreter web application
- Interpreter Chrome browser extension
- Interpreter backend server
- Database for user and session data
- Integration with the speech recognition provider
- Integration with Google OAuth for authentication
- Integration with Dodo Payments for billing

Subservice organizations — Interpreter relies on a certified speech recognition provider and managed cloud providers for hosting. The speech recognition provider's SOC 2 Type II report covers its infrastructure independently.

Security controls

Organization and management

Interpreter maintains security policies governing access to production systems and incident response. Since Interpreter does not store audio or transcripts, the data footprint is limited to account information. Production access is restricted to authorized personnel.

Access control

- User authentication through Google OAuth 2.0 with session cookies
- Automatic session expiry
- Secure session cookies (HttpOnly, Secure, SameSite)
- Users are isolated to their own data
- Production infrastructure access restricted to the engineering team
- Secrets managed through Infisical, not stored in source code

Network security

- All external communication over TLS

- CORS policy restricting API access to authorized origins
- Rate limiting on all API endpoints
- Webhook signature verification for payment provider callbacks

Data protection

- No audio or transcript data stored on Interpreter's servers
- The only stored data is account information (email, name) and session duration
- Database connections encrypted in transit
- Payment card data handled entirely by PCI-compliant payment processor (Dodo Payments)
- Account deletion removes all associated data

Monitoring and incident detection

- Automated detection and termination of inactive sessions
- Rate limit violation tracking
- Logging of system activity and access events
- Automated inactivity detection with session termination

Change management

- Source code managed in version control
- Containerized deployment
- Environment configuration validated at startup

Availability

- Automated session cleanup prevents resource exhaustion
- Session monitoring with automatic recovery
- Reconnection with exponential backoff for network interruptions
- Graceful handling of speech engine disconnections

Vendor management

Interpreter assesses the security posture of third-party providers before integration. The speech recognition provider holds SOC 2 Type II and ISO/IEC 27001:2022 certifications. The payment processor (Dodo Payments) is PCI-compliant. Cloud infrastructure providers maintain their own SOC 2 certifications.

Subprocessor certifications

The speech recognition provider holds:

- SOC 2 Type II — Independently audited with a clean opinion covering the trust service criteria for Security
- ISO/IEC 27001:2022

Copies of both documents are available upon request.

Complementary user entity controls

Interpreter's security controls assume that customers implement certain controls on their end:

- Protecting their account credentials and not sharing login sessions
- Using the platform in compliance with applicable laws and regulations
- Reporting suspected security incidents promptly

Contact

For security-related questions or to request copies of subprocessor certifications:

Interpreter Security and Compliance security@useinterpreter.com