INTERPRETERCONNECT SECURITY FAQ

At All Languages, safeguarding your sensitive data and ensuring privacy are our top priorities. We are committed to industry-leading security practices so you can confidently use our platform.

Table of Contents

ACCESS CONTROL

How does your product manage user accounts (provisioning, deprovisioning, reviews)?

Our intuitive Admin Portal empowers customer admins and call center managers to easily create, update, or deactivate interpreter accounts. Deactivation requests are efficiently processed through support tickets.

Does the product enforce role-based access control (RBAC) or other access control mechanisms?

We assign roles to admin users at account creation, ensuring that each user's access is tailored to their responsibilities. Admins can adjust these roles as needed, so users only see relevant features.

Does the product implement account lockout after failed login attempts?

Account lockout is not currently implemented. Please contact us for custom security options.

Does the product support inactivity timeout for a certain period of time?

Yes, the system automatically logs out users after periods of inactivity, enhancing session security.

How does the product manage access from mobile devices?

InterpreterConnect delivers identical security and functionality across desktop, tablet, and mobile devices, ensuring a seamless browser-based experience.

AUDIT & ACCOUNTABILITY

What events are logged by the product (e.g., logins, data access, changes)?

Our system logs all key events, including logins, logouts, data access, and live call requests, supporting robust monitoring and accountability.

What information is included in audit logs (timestamps, user IDs)?

Audit logs capture timestamps, user IDs, IP addresses, application, and operating system details for a comprehensive history.

Does the product provide tools for reviewing and analyzing audit logs?

Internal tools are available for thorough audit log review and analysis, enabling proactive security checks.

Can the product generate compliance and security audit reports?

Yes, we provide compliance and security audit reports as needed.

How does the product synchronize system time for accurate logging?

Audit logs synchronize with the operating system, ensuring accurate timestamps and consistent reporting.

IDENTIFICATION & AUTHENTICATION

What forms of identification and authentication does the product support? Is MFA offered?

We use JWT tokens, IP whitelisting, and access codes for secure identification and authentication. Multi-factor authentication protects internal network access.

How are user identifiers managed to ensure they are unique?

Each user session is assigned a unique identifier and JWT token, guaranteeing session accuracy and security.

How does the product handle authentication mechanisms (passwords, tokens)?

Our platform follows industry-standard encryption, including secure passwords, tokens, and AES-128/AES-256 encryption to protect authentication processes.

How are non-organizational users (e.g., third-party contractors) authenticated and managed?

All users have unique usernames and passwords, with accounts managed by our internal call center admin team for added oversight.

SYSTEM & COMMUNICATIONS PROTECTION

How does the product secure data during transmission (e.g., TLS, IPSec)?

Data in transit is encrypted with AES-128 and AES-256 standards, including TLS and IPSec protocols for comprehensive security.

What cryptographic methods does the product use for data encryption and key management?

We utilize AES-128 and AES-256 encryption for both transmitted and stored data to ensure sensitive information remains protected.

Does the product encrypt sensitive data at rest? What standards are used?

Sensitive data at rest is safeguarded using AES-128 and AES-256 encryption.

SYSTEM & INFORMATION INTEGRITY

How frequently are patches and updates applied to address security vulnerabilities?

We promptly apply patches based on vulnerability severity. Last year, three major updates addressed identified vulnerabilities.

How does the product ensure the integrity of software, firmware, and data (e.g., using checksums)?

Checksum verification is implemented in package-lock files to maintain software and data integrity.

CONFIGURATION MANAGEMENT

Is there a change management process for making configuration changes?

All configuration changes are tracked via structured change controls, supporting thorough management and oversight.

How does the product minimize the attack surface (disable unnecessary services, ports)?

Our internal network is protected by multi-factor VPN authentication, firewalls, and digital certificates to minimize risk.

CONTINGENCY PLANNING

Does the product have a contingency plan for recovery in the event of a failure or disaster?

Yes, a comprehensive contingency plan is in place to enable rapid recovery from any failure or disaster.

Does the product support alternate data storage and backup locations?

We perform daily backups to both Google Cloud and Azure, ensuring data redundancy and accessibility.

How does the product handle data backups? Are backups automated and encrypted?

Backups are fully automated and encrypted using AES-256 standards.

INCIDENT RESPONSE

How are incidents reported to stakeholders or regulatory bodies?

Our critical incident response team manages communications with all affected parties, including regulatory and customer stakeholders.

RISK ASSESSMENT

How often are risk assessments conducted to identify potential vulnerabilities?

Risk assessments occur regularly and vulnerability scans are performed daily to ensure ongoing protection.

Does the product support regular vulnerability scanning?

Yes, daily vulnerability scanning is part of our routine security process.

MEDIA PROTECTION

How is sensitive data protected during transport? Is encryption used?

Data is encrypted during transit using TLS, with comprehensive protection for media files.

SECURITY ASSESSMENT & AUTHORIZATION

Does the product undergo regular security assessments?

We conduct penetration tests and can provide the latest assessment reports upon request.

How are security deficiencies tracked and addressed?

Security issues are logged in Prisma Cloud and internal ticketing systems, ensuring timely resolution.

SUPPLY CHAIN RISK MANAGEMENT

How are third-party vendors and suppliers assessed for security risks?

Third-party vendors undergo security reviews and are subject to VPN and firewall restrictions.

Are security requirements included in contracts with suppliers?

Yes, all supplier contracts include robust security requirements.

PRIVACY CONTROLS

How does the product handle personally identifiable information (PII)?

PII is encrypted at rest in our secure database, following industry best practices.

MAINTENANCE

How are maintenance activities documented and tracked?

Maintenance activities are tracked through our change controls and ticketing platform for reliable documentation.

How are maintenance tools secured to prevent unauthorized use?

We are happy to discuss further once we clarify your definition of maintenance tools.

ADDITIONAL QUESTIONS

Does the product comply with recognized security certifications (e.g., FedRAMP, ISO 27001)?

We adhere to NIST security standards throughout our processes.

Has the product undergone third-party audits? If yes, can you provide reports?

We regularly complete customer audits and questionnaires, such as SIG Lite. Reports are available upon request.

How is security maintained for products reaching end-of-life?

End-of-life products are securely decommissioned and replaced with newer, licensed devices.

Does the product comply with relevant regulations (e.g., GDPR, HIPAA, CCPA)?

Yes, we comply with GDPR, HIPAA, and CCPA, ensuring rigorous data protection for all users.