Information Security Program

We have an Information Security Program in place that is communicated throughout the organisation. Our Information Security Program follows the criteria set forth by the ISO27001 Framework. ISO27001 is a widely known information security management system certification that is internationally recognised.

Third-Party Audits

Our organisation undergoes independent third-party assessments to test our security and compliance controls. This process is handled annually.

Third-Party Penetration Testing

We perform an independent third-party penetration at least annually to ensure that the security posture of our services is uncompromised.

Roles and Responsibilities

Roles and responsibilities related to our Information Security Program and the protection of our customer's data are well defined and documented. Our team members are required to review and accept all of the security policies.

Security Awareness Training

Our team members are required to go through mandatory security awareness training covering industry standard practices and information security topics such as phishing and password management.

Confidentiality

All team members are required to sign and adhere to an industry standard confidentiality agreement prior to their first day of work.

Background Checks

We perform background checks on all new team members in accordance with local laws.

Cloud Security / Cloud Infrastructure Security

All of our Straker LanguageCloud services are hosted with the IBM Cloud Platform in Europe. They employ a robust security program with multiple certifications including ISO27001 and SOC2. For more information on our provider's security processes, please visit IBM Cloud Security.

Data Hosting Security

All of our data is self-hosted within a private cloud using IBM Cloud infrastructure. These databases are all located in Europe.

Encryption at Rest

All databases are encrypted at rest.

Encryption in Transit

Our applications encrypt in transit with TLS/SSL with a minimum of TLS v1.2.

Vulnerability Scanning

We perform regular vulnerability scanning and actively monitor for threats.

Logging and Monitoring

We actively monitor and log various cloud services.

Artificial Intelligence (AI) Usage

We leverage closed-loop AI systems to enhance operational efficiency and decision-making, ensuring strict control over data inputs and outputs. We do not use public AI tools or models, aligning all AI-driven processes with our internal policies and ethical standards. Straker integrates AI into our translation services, combining generative AI with human expertise to provide fast and accurate translations. Our AI verification ecosystem supports businesses in creating localized content for global markets, ensuring high-quality translation support across various languages and industries. This hybrid approach allows us to leverage the benefits of AI while maintaining ensuring data security, compliance, and accuracy through rigorous human oversight.

Business Continuity and Disaster Recovery

We maintain several backup services to reduce any risk of data loss in the event of a hardware failure. Our disaster recovery backup system is fully encrypted and geographically separate from the production datacenter. We utilise monitoring services to alert the team in the event of any failures affecting users.

Incident Response

We have a process for handling information security events which includes escalation procedures, rapid mitigation and communication.

Access Security

Permissions and Authentication

Access to cloud infrastructure and other sensitive tools are limited to authorised employees who require it for their role, observing a least-privileges approach with respect to identity and access management. Where available we have Single Sign-on (SSO), 2factor authentication (2FA) and strong password policies to ensure access to cloud services and systems are protected.

Quarterly Access Reviews

We perform quarterly access reviews of all team members with access to sensitive systems.

Password Requirements

All our applications adhere to a set of defined password requirements (length and complexity) for access.

Password Managers

Password managers are used by staff to manage unique personal and team passwords and maintain password complexity.

Vendor and Risk Management

Annual Risk Assessments

We undergo at least annual risk assessments to identify any potential threats, including considerations for fraud.

Vendor Risk Management

Vendor risk is determined and the appropriate vendor reviews are performed prior to authorising a new vendor.

Quarterly Access Reviews

We perform quarterly access reviews of all team members with access to sensitive systems.

Contact Us

If you have any questions, comments or concerns or if you wish to report a potential security issue, please contact security@strakergroup.com.