AI Bloks Security

At AI Bloks, we believe that security is a responsibility we share with our users. We empower our users with easy-to-use features that provide auditability along with complete control over who can access their data.

We have a robust Information Security Program in place that is communicated throughout the organization. We have achieved SOC 2 Type 2 compliance, which means that the design of our security controls and their operational effectiveness have been evaluated by an external auditor, Insight Assurance.

The SOC 2 Framework is a widely known information security auditing procedure created by the American Institute of Certified Public Accountants.

Our Program follows the criteria set forth by the SOC 2 Framework:

Third-Party Audits
Our organization undergoes independent third-party assessments to test our security and compliance controls.

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 employee 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 Infrastructure Security

All of our services are hosted with Amazon Web Services (AWS) which employ a robust security program with multiple certifications. For more information on our provider's security processes, please visit AWS Security.

Data Hosting Security

All data is hosted on Amazon Web Services (AWS). All data storage is located in the United States.

Encryption at Rest

All data are encrypted at rest.

Encryption in Transit

Our applications encrypt in transit with TLS/SSL only.

Vulnerability Scanning

We perform ongoing host-based vulnerability scans.

Logging and Monitoring

We actively monitor and log various cloud services.

Business Continuity and Disaster Recovery

We use backup services to reduce any risk of data loss in the event of a hardware failure.

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 authorized employees who require it for their role. Where available we have Single Sign-on (SSO), 2-factor authentication (2FA) and strong password policies to ensure access to cloud services are protected.

Least Privilege Access Control

We follow the principle of least privilege with respect to identity and access management.

Quarterly Access Reviews

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

Password Requirements
All team members are required to adhere to a minimum set of password requirements and complexity for access.

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
We perform a risk assessment on all vendors and appropriate reviews are performed prior to authorizing a new vendor.

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

Contact Us

If you'd like to request our SOC 2 report or if you wish to report a potential security issue, please contact us.