EliseAI Security & Compliance Overview

EliseAI

We are committed to ensuring the confidentiality, integrity, and availability of our systems and customer data. Our security program is designed around industry best practices and robust internal controls. Our SOC 2 Type II and HIPAA reports are available upon request.

Infrastructure & System Security

Unique Authentication Enforced
Access to production systems requires unique credentials and/or secure SSH keys.

Privileged Access Restricted
Production databases, firewalls, operating systems, and networks are only accessible to authorized personnel with a business need.

Encryption
Data is encrypted at rest with minimum AES-256 and during transmission with minimum TLS v1.2.

Intrusion Detection & Network Segmentation
Continuous monitoring and segmented networks safeguard against unauthorized access.

System Hardening & Firewall Management
Industry-standard hardening practices and annually reviewed firewall configurations are enforced.

Organizational Security

Access Control Policies
Formalized procedures for user provisioning, modification, and deprovisioning.

Multi-Factor Authentication (MFA)
MFA is mandatory for all remote access to production systems.

Asset & Media Management
Inventory is maintained; portable media is encrypted; asset disposal is securely handled with certificates of destruction.

HR Safeguards
Background checks conducted; employees and contractors sign confidentiality and code of conduct agreements.

Mobile Device Management
Centrally managed employee workstations via MDM.

Audit Logging
All user activity, administrative actions, system changes, and other auditable events are logged and stored per regulatory requirements.

Security Awareness
All employees attend security awareness and PHI handling training upon hire and annually thereafter.

Insurance
Customary cyber incident insurance is held.

Product & Application Security

Penetration Testing
Annual tests with remediation plans.

Vulnerability & Monitoring Procedures
Formal policies for regular system checks and updates.

Secure Development Lifecycle
Code changes undergo testing, review, and approval before deployment.

Internal Operations

Change & Configuration Management
Controlled, documented, and authorized changes to infrastructure.

Business Continuity & Disaster Recovery
Plans in place and tested annually to ensure resilience.

Incident Response
Policies and procedures documented, tested annually, and followed for security events.

Access Reviews & Requests
Quarterly access reviews; access requests are role-based and require manager approval.

Support Systems
Robust internal and external support channels are available.

Governance & Compliance

Risk Management
Ongoing assessments with documented mitigation strategies.

Third-Party & Vendor Controls
Business Associate Agreements (BAA), privacy requirements, and annual vendor reviews are maintained with vendors as required by law.

Regulatory Alignment
All controls are aligned with SOC 2 standards and other relevant compliance frameworks.

Data Governance
Retention, classification, and deletion procedures are in place to protect customer data and to meet regulatory requirements.

U.S. Location
All customer data remains within the United States of America including data processed by any subprocessors.

No Sale of Data
Customer data is never sold to third parties.

AI Governance & Risk

Quality Assurance
A system of heuristics will automatically flag AI responses or actions that deviate from a norm for human review.

No LLM Training
Your data is not used to train any Large Language Models (LLM).