Security

Closinglock is a leading provider of fraud prevention technology in real estate, offering a secure, easy-to-use platform that connects settlement companies with buyers, sellers and lenders. With its firm commitment to safeguarding customer data, Closinglock employs the latest technology and adheers to the highest industry standards.

This document serves as an introduction to Closinglock's comprehensive approach to security, highlighting the systems and policies currently in place.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

How We Protect Your Data

Closinglock relies on ISO 27001 and SOC 2-certified data centers. These data centers are expertly managed by Amazon Web Services (AWS) to host all web servers, associated file storage, and databases. Data stored within AWS is redundantly backed up to ensure resilience and uninterrupted service levels.

Access to AWS is fortified with strong, unique passwords and two-factor authentication (2FA). All data is encrypted in transit and at rest, employing state-of-the-art AES 256-bit encryption.

Network and Application Security

Closinglock deploys Cloudflare as a web application firewall, utilizing "High/Secure" configurations where applicable. Access to Cloudflare is protected by robust passwords and 2FA through a dedicated app, with regular checks on settings, configurations and logs.

To guarantee secure connections, TLS/SSL is mandatory for all interactions throughout the site and network. Additionally, SSH access to Closinglock's network is restricted to a predefined set of whitelisted IP addresses. Firewall rules are also employed to block access from OFAC-sanctioned countries.

SOC 2 Compliance

Closinglock is proud to announce that we are SOC 2, Type 2 compliant. This certification demonstrates our commitment to adhering to the highest standards of security, availability, processing integrity, confidentiality, and privacy controls.

Business Continuity

Closinglock conducts regular business continuity tests:

- **On-site systems** undergo monthly updates and are equipped with active, up-to-date virus and malware scanning
- **Hosted systems** utilize a multi-zone deployment strategy where applicable, ensuring redundancy. Backup and restoration procedures are set up for both web servers and databases, with a Recovery Time Objective (RTO) of 24 hours.
- **Web servers** are restored using EC2 backup images from AWS, while database instances are recovered using RDS backup images from AWS. Our Web Application Firewall (WAF) can swiftly deploy "under attack" mode through Cloudflare.

Policies and Programs

Closinglock maintains an extensive array of internal policies and programs to fortify our security posture, including but not limited to:

- Acceptable Use
- Access Control
- Backup and Restoration
- Change Management
- Data Retention and Disposal
- Information Security
- Network Security
- Privacy
- Third-Party Risk Management

Closinglock

sales@closinglock.com | closinglock.com