LENDBOX

Security at Lendbox

Lendbox is the system of record for lending institutions. This page describes how we protect the borrower and portfolio data our customers trust us with, the controls available inside the product, and the third parties involved in delivering the service.

Last reviewed 2026-09-01. This page is reviewed against the running system, not on a schedule.

ON THIS PAGE

1. Data protection

> Lendbox runs on Amazon Web Services in the us-east-1 region, United States. The application, the database, and uploaded documents in Amazon S3 are all in that region.

> Data is encrypted in transit using TLS 1.3.

> Data is encrypted at rest using AES-256. Database and application storage volumes are encrypted with AWS EBS encryption. Uploaded documents and backups are encrypted with server-side encryption in Amazon S3. Encryption keys are managed through AWS Key Management Service.

> Customers can export their full data set at any time from within the product. No request to us is required.

> **On account closure, customer data is retained for 60 days and then permanently deleted. During that window the account can be restored on request.**

2. Infrastructure

> Application and database run on isolated AWS infrastructure. Databases are not publicly reachable and accept no connections from the internet. The web tier is served by Vercel.

> All inbound traffic passes through Cloudflare, which provides DDoS mitigation and a web application firewall.

> Environments are separated: production, staging and development run on separate infrastructure with no shared credentials. Development and staging contain no production data.

3. Access control inside the product

The controls in this section are operated by the customer, not by us. An institution configures them itself, and can verify at any time what each staff member can do.

> Graduated per-module permissions. Every module can be set per staff member to one of six levels, shown below.

> Multi-branch role assignment. A single staff account can be granted access to multiple branches and hold a different role in each, so a branch manager in one location is a view-only user in another.

> Maker-checker separation. Sensitive actions are split between the staff member who requests them and the staff member who approves them. Approval workflows are configurable per institution, including the number of approval steps and which roles can act at each step.

> Multi-factor authentication. Available on every login, and can be enabled independently by each individual user and staff member.

> Login sessions expire after 5 days and require re-authentication.

Permission levels

Each module is set independently, per staff member.

None

The module is not available and does not appear in the staff member's navigation.

View Only

Can open and read records. Cannot change anything.

Can Request

Can submit an action for approval. Cannot approve it.

Can Approve

Can approve actions submitted by other staff members.

Can Edit

Can create and change records directly.

Has Access

Full access, for modules that are not split into request and approve steps.

4. Audit trail

> Every action taken in the product is recorded with the acting user, the affected record, and a timestamp.

> Audit records are append-only. They cannot be edited or deleted from the application, including by institution administrators.

> Closed accounting periods are locked against retroactive modification.

> Institution administrators can export the audit history at any time.

Audit history is retained for the full life of the account, from the date it was created. There is no rolling window and no truncation.

5. Backups and recovery

Databases are backed up every hour.

Backups are encrypted and retained for 6 months.

Recovery point objective (RPO): 1 hour.

Restores are tested weekly against a non-production environment. A backup that has not been restored is not a backup.

6. Internal access and secrets

Access to production data is limited to a single named individual, the founder. No other employee, contractor, or third party holds production credentials. This is a deliberate design decision: it is the smallest possible surface area of people who can reach customer data.

Production access is individually credentialed and protected by multi-factor authentication. No shared accounts or credentials are used anywhere in the organisation.

Application secrets and credentials are managed in Doppler. They are not stored in source control or on developer machines.

> Continuity: a documented break-glass procedure covers the case where the individual holding production credentials is unavailable. Recovery credentials are held in sealed escrow with a named second party, released on a defined trigger, and every use is logged. The procedure restores customer access to their own data; it does not grant standing access to anyone.

7. Vulnerability and patch management

Security vulnerabilities are remediated on severity-based targets, measured from the point the vulnerability is confirmed as affecting Lendbox.

> Application dependencies are monitored continuously with Renovate, which opens patch pull requests automatically as upstream releases are published.

> Dependency updates are reviewed and merged on a weekly cycle. Advisories with a known exploit bypass that cycle and are raised immediately.

> Operating system and container base images are rebuilt and redeployed on a monthly cadence, and immediately on disclosure of a critical vulnerability.

Remediation targets

Severity	Remediation target
Critical	48 hours
High	7 days
Medium	30 days
Low	Next scheduled release cycle

8. Subprocessors

The services listed here process data on our behalf under contract.

Subprocessor	Purpose	Data accessed	Location
Amazon Web Services	Application hosting and database	All customer and borrower data	United States (us-east-1)
Amazon Web Services (S3)	Document and backup storage	Uploaded documents, database backups	United States (us-east-1)
Vercel	Web application hosting and delivery	Request metadata, IP address	United States, global edge
Cloudflare	DNS, CDN, DDoS mitigation, web application firewall	Request metadata, IP address	Global edge
Google Firebase	Staff authentication, including multi-factor	Staff name, email address, authentication tokens	United States
Doppler	Application secret and credential management	No customer data. Service credentials only.	United States
Paddle	Card subscription billing, merchant of record	Institution billing contact and payment details	United Kingdom
Lenco	Mobile money subscription payments	Institution billing contact, transaction reference	Zambia
PostHog	Product analytics and feature flags	Staff user identifier, email address, in-product events	United States
Bugsnag (SmartBear)	Application error reporting	Staff user identifier, error diagnostics	United States
OneSignal	Web and mobile push notifications	Device token, staff user identifier	United States

Typesense	In-product search index	Navigation and help content. No borrower data.	United States
OpenRouter	Model routing for in-product AI features	The text of a query a staff member submits	United States
Google reCAPTCHA	Bot protection on authentication forms	IP address, browser signals	United States
Google Tag Manager	Marketing tag management on the public website	Website visitor analytics. No product data.	United States

Customers are notified by email at least 30 days before a new subprocessor is added or an existing one is replaced, at the administrative contact on the account.

Self-hosted components

The following run on infrastructure we control. They are named because they are visible to anyone inspecting the product, but they are not subprocessors: no third party receives data through them.

Component	Purpose	Host
Chatwoot	Support chat	support.lendbox.io
Seq	Application logging	logs.lendbox.io
Shlink	Short links for document signing	s.lendbox.io
Squidex	Marketing content management. No product data.	cms.popsicleai.com

9. Monitoring and incident response

> Infrastructure and application health are monitored continuously using Prometheus, Alertmanager, and cAdvisor, with alerts routed to an on-call engineer.

> In the event of a security incident affecting customer data, affected customers are notified within 72 hours of confirmation. Notifications state what happened, which data was affected, what we have done to contain it, and what action, if any, the customer needs to take.

> Availability incidents are posted to the status page as they are being worked on, not after resolution.

Uptime and incident history are public
Every service has 90 days of daily status and the duration of every outage published at status.lendbox.io. We publish outages rather than hiding them.
https://status.lendbox.io/

10. Reporting a vulnerability

> Email security@lendbox.io. Include steps to reproduce.

> We acknowledge every report within 3 business days, and give an assessment of severity and expected remediation timeline within 10 business days.

> We do not pursue legal action against researchers who report in good faith, avoid privacy violations and service degradation, and give us reasonable time to remediate before disclosure.

> Our machine-readable contact details are published at /.well-known/security.txt.

security@lendbox.io · https://lendbox.io/en/security · 2026-09-01