BOORDS

Security Overview

LAST UPDATED	CONTACT	OWNER
3 November 2026	hello@boords.com	James Chambers, Data Privacy Manager

---

A summary of Boords' security and data protection posture, intended for procurement, IT, and security reviewers.

1. About Boords

Boords is the pre-production platform for video agencies and in-house brand teams, used to plan, storyboard, animate, and approve video projects.

The service is operated by:

Presentable Software Limited (trading as Boords) Unit A St Andrews Court, Wellington Street, Thame, England, OX9 3WT, United Kingdom Company registered in England and Wales (company number 09985153) Registered with the UK Information Commissioner's Office (ICO)

For all security and data protection enquiries, contact hello@boords.com.

2. Hosting and infrastructure

Boords runs on managed infrastructure from established cloud providers. Boords does not operate any self-managed servers.

COMPONENT	PROVIDER	REGION
Application hosting	Heroku (a Salesforce company)	EU (Ireland)
Database (PostgreSQL)	Heroku Postgres	EU (Ireland)
File storage	Amazon Web Services (S3)	EU (Ireland)
Image processing	AWS Lambda	EU (Ireland)
Edge, CDN, WAF, DDoS protection	Cloudflare (app.boords.com)	Global

Cloudflare sits in front of the main web application (app.boords.com), providing web application firewall protection with automatically updated rulesets, traffic filtering, and DDoS mitigation at the network and application layers. The API (api.boords.com), the real-time collaboration service and custom team subdomains connect directly to Heroku and are not proxied by Cloudflare. AWS and Heroku provide platform-level DDoS countermeasures as part of their managed infrastructure, and the application applies per-IP and per-account rate limits to API and team-subdomain requests.

3. Encryption

In transit. All access to Boords is restricted to 256-bit SSL encrypted connections (HTTPS). Older insecure protocol versions are not supported. Boords uses valid SSL certificates issued by a trusted certificate authority and managed via Heroku and Cloudflare.

At rest. Files stored on AWS S3 are encrypted at rest using server-side encryption with AWS S3-managed keys (SSE-S3), automatically applied to all objects. Backup data on AWS S3 is encrypted to the same standard.

Key management. Encryption key management is fully delegated to the underlying infrastructure providers (AWS and Heroku). Keys are managed, rotated, and maintained by the respective platform providers.

4. Access control

Principle of least privilege. Access to production systems, infrastructure, and repositories is restricted to Boords staff and authorised contractors with a specific business need. Access rights are reviewed when staff or contractors join or leave.

Customer data. Access to deposited customer data by Boords staff is prohibited in principle. In exceptional circumstances (e.g. support or debugging), access is taken only with the explicit prior consent of the customer and is limited to the minimum data necessary.

Privileged accounts. Privileged access to production infrastructure (AWS, Heroku, database) is held only by named individuals. Any access granted to contractors is scoped to the minimum required for the specific engagement and revoked on completion. Default credentials are never used; strong unique passwords are enforced via a password manager.

Customer-facing roles. Customer team accounts have a role model of Admin, Manager, Supermember, and Member. Sharing permissions, API token management, and team administration are scoped to the appropriate roles.

5. Authentication

Customer accounts. Boords provides native email-and-password authentication for all customers, with Google OAuth also available. Multi-factor authentication is available via an authenticator app. Passwords are hashed using bcrypt with a unique salt. A minimum password length and complexity is enforced and the use of compromised passwords is restricted. Login attempts are rate-limited to prevent brute-force attacks. User sessions expire after seven days of inactivity.

Administrative accounts. Access to Boords' AWS and Heroku consoles is protected by multi-factor authentication. Administrative sessions are subject to platform-enforced session timeouts.

6. Logging and monitoring

Uptime. Service performance and uptime is monitored via Pingdom with alerting enabled. A public status page is maintained at status.boords.com.

Application logs. Application logs are forwarded to New Relic and retained for 30 days. Errors and exceptions are recorded in New Relic and Rollbar. AWS CloudWatch retains infrastructure logs.

Access logs. Access to AWS and Heroku management interfaces is monitored via platform-provided access logs and protected by MFA-enforced administrative consoles.

Time synchronisation. Time is synchronised via NTP across all service components by AWS and Heroku managed infrastructure.

7. Backup, recovery, and resilience

Database backups. Heroku Postgres takes daily backups, retaining seven daily and four weekly copies. A separate daily backup is stored outside Heroku in encrypted AWS S3 storage in Stockholm, with 30-day Object Lock protection. Heroku continuous protection provides point-in-time recovery for the previous four days; this is separate from the daily backups.

File backups. Files stored on AWS S3 carry built-in redundancy and data durability across multiple availability zones within the EU (Ireland) region.

Application code. All application code is version-controlled via Git with a full audit trail of changes, authors, and timestamps.

Database recovery. A documented production Postgres recovery runbook covers damaged or deleted data, primary database failure, and loss of Heroku access or the hosting region. It records recovery targets, operator responsibilities, restore procedures, and drill results. An off-Heroku backup has been restored and verified, and a point-in-time recovery copy has been created and checked. Full database promotion, primary-failure recovery, and the complete loss-of-Heroku recovery procedure have not been drilled end to end.

Resilience scope. The production application and primary database are hosted in a single region (EU Ireland). A database follower supports manual recovery; automatic failover and a complete business continuity plan covering re-hosting the application remain gaps. The database runbook does not establish a fully tested recovery process for every scenario. See section 14 below.

8. Network security

Perimeter protection. Cloudflare provides edge filtering, WAF, and DDoS protection in front of the main web application (app.boords.com). The API, the real-time collaboration service and custom team subdomains are served directly by Heroku, with Heroku's platform-level DDoS protection; the application rate-limits API and team-subdomain requests per IP address and per account.

Database isolation. The Heroku Postgres database is logically separated from the application server. Communication between the application and database is restricted to Heroku's internal private networking. Direct access to the database is restricted to authorised administrators only.

Port exposure. Only HTTPS (443) is exposed publicly, via Cloudflare for the main web application and via Heroku's router for the other hostnames. Unnecessary ports are closed by default on Heroku and AWS managed infrastructure.

9. Development and deployment

Environments. Separate development, staging, and production environments are maintained on Heroku. Production data is not used in non-production environments.

Version control. All code changes are tracked via Git with a full audit trail of changes, authors, and timestamps.

Testing. Automated functional and static-analysis tests are run via the CI pipeline on every change before deployment. Changes are tested in the staging environment before being released to production.

Deployment authority. Service releases and deployments are performed by authorised personnel only.

Dependency management. Open-source dependencies are managed via Bundler (Ruby gems) and npm. Application-level updates and security patches are applied as needed. OS, middleware, and platform security patches are applied automatically by the underlying infrastructure providers.

10. Sub-processors and international transfers

Boords engages the following named sub-processors. All sub-processors are bound by data processing agreements and may only process data on Boords' instructions.

SUB-PROCESSOR	PURPOSE	REGION	TRANSFER MECHANISM
Amazon Web Services	File storage, infrastructure, backups	Ireland and Sweden (EU)	N/A
Heroku (Salesforce)	Application hosting, PostgreSQL database, Redis	Ireland (EU)	N/A
Cloudflare	Edge, CDN, WAF, DDoS (main web application)	Global	SCCs
MemCachier	Application caching	Ireland (EU)	N/A
Pusher	Real-time collaboration updates	Ireland (EU)	N/A
Stripe	Payment processing	United States	SCCs
Postmark	Transactional email	United States	SCCs
Intercom	Customer support messaging	United States	SCCs
Mailerlite	Marketing email	Lithuania (EU)	N/A
Google Analytics	Web analytics	United States	SCCs
PostHog	Product analytics	Germany (EU)	N/A
OpenAI	AI script import, image generation, moderation	United States	SCCs
Fal.ai	AI image generation	United States	SCCs
Google (Gemini API)	AI image generation and AI assistant	United States	SCCs
Google sign-in	Optional single sign-on	United States	SCCs
Filestack	File storage and processing	United States	SCCs
Transloadit	Image processing and upload	United States	SCCs
Cloudinary	Audio upload and processing	United States	SCCs
ipstack (apilayer)	IP geolocation for billing currency	Austria (EU)	N/A
Canny	Product feedback and changelog	United States	SCCs
New Relic	Performance monitoring, error tracking, server logs	United States	SCCs
Rollbar	Error tracking	United States	SCCs

SUB-PROCESSOR	PURPOSE	REGION	TRANSFER MECHANISM
Google Workspace	Company email, including support correspondence	United States	SCCs
Anthropic	Staff AI assistant (engineering and support)	United States	SCCs
xAI	Staff AI assistant (support investigations)	United States	SCCs

Where data is transferred outside the EEA, Boords relies on the European Commission's Standard Contractual Clauses (SCCs). All sub-processors are evaluated prior to engagement and required to maintain appropriate safeguards.

11. Data subject rights

Boords complies with the UK GDPR and aligns with the EU GDPR and CCPA/CPRA. Customers and data subjects have the following rights:

- Right to access their personal data
- Right to correction
- Right to erasure
- Right to object to processing
- Right to restrict processing
- Right to data portability
- Right to withdraw consent

Requests are handled within one month, as required by UK GDPR, and may be submitted by email to hello@boords.com. By law, basic customer data (identity, contact, financial, and transaction data) is retained for six years after account closure to satisfy UK legal and tax obligations.

Data export. Customers can export their storyboards directly from the Boords application in PDF, image, and animatic formats at any time.

Account deletion. Customers can request account deletion at any time, with personal data erased within one month of request (subject to legal retention obligations).

12. Email security

All transactional and notification email is sent from the boords.com domain via Postmark with SPF, DKIM, and DMARC configured to prevent spoofing and impersonation.

13. AI features and data handling

Boords integrates external AI services to power the following features:

- **Script import and storyboard generation:** OpenAI
- **AI image generation:** Fal.ai, Google (Gemini API), OpenAI
- **Image prompt moderation:** OpenAI
- **AI assistant:** Google (Gemini API)

Boords does not train, retrain, or fine-tune any AI or machine learning models using customer data. Customer content submitted to the AI services listed above is also not used to train the underlying models, per the providers' API terms.

Account-level opt-out. Account admins can disable AI features for the entire account from account settings. When disabled, no AI processing runs for any user on the account.

Boords' Terms of Use include a Fair Use policy for AI image generation, covering acceptable use, usage limits, and enforcement measures.

14. Compliance, frameworks, and roadmap

Current standing.

- UK GDPR compliant
- Registered with the UK Information Commissioner's Office (ICO)
- Aligned to EU GDPR and CCPA/CPRA
- Completed the Assured SaaS Security Risk and Trust Assessment (April 2026)

Compensating controls. Where Boords does not hold a specific framework certification, the underlying managed infrastructure (AWS, Heroku, Cloudflare, Stripe) carries equivalent certifications including SOC 2, ISO 27001, and PCI DSS. These provide the platform-level security controls on which Boords is built.

Not currently certified. Boords is not directly certified to SOC 2 or ISO 27001 today. Boords is preparing for a SOC 2 Type 2 audit.

Implemented.

- Weekly external vulnerability scanning of Boords' internet-facing hosts, in place since October 2026

In progress.

- Formal information security policies (including access control, change management, incident response, vulnerability management, vendor management and business continuity): approval, publication and staff sign-off before our SOC 2 observation period begins
- Background screening and security awareness training for current personnel: before our SOC 2 observation period begins
- Complete business continuity planning beyond the documented Postgres recovery runbook, including application re-hosting and the remaining recovery drills: next drill planned during our SOC 2 observation period

This document will be updated as these items are completed.

15. Incident response and breach notification

Accountability. The data privacy manager (James Chambers, james@boords.com) is the named individual accountable for security incident response and personal data breach handling.

Breach notification. In the event of a personal data breach, Boords will notify affected users and the UK Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where legally required under UK GDPR. Notification to affected users is made by email.

Incident communication. Service-affecting incidents are communicated via status.boords.com, the in-app notification system, and (where applicable) by email.

Reporting a vulnerability. Suspected vulnerabilities may be reported to hello@boords.com. We will acknowledge reports and work in good faith with the reporter to resolve issues. We request a reasonable window for investigation and remediation before public disclosure.

16. Document control

Owner	James Chambers, Data Privacy Manager
Contact	hello@boords.com
Last updated	2026-11-03
Next review	2027-05-26
Distribution	Public. May be shared freely with prospects, customers, and procurement teams.