

TRUST & PROCUREMENT

Security & *confidentiality*

How Boardmate is built and operated to protect confidential board material: controlled workspaces, scoped review, managed cloud infrastructure, protected AI-assisted drafting, auditability, retention, and the private security pack your team can review.

How we think about confidential board work

Board packs, transcripts, draft minutes, and reviewer feedback are sensitive. This overview is written for the people who evaluate that risk. It is a plain-language summary; deeper documentation is available on request before confidential material moves.

Workspaces & named users

Each customer works in a private, logically separated workspace. Authorised users are named and keep control of source material, drafts, decisions, export, and deletion.

Audit trail

Access, opens, comments, uploads, no-comment confirmations, moderation, regeneration, exports, and downloads are recorded against the meeting.

Reviewer links

Attendees and service providers review through scoped private links – recipient-specific, revocable, and expiring – rather than broad workspace accounts.

Human control

Reviewer feedback is input, not authority. The chair or delegated owner decides what shapes the next draft. Learned house style affects wording only, never the facts of a meeting.

A controlled platform for confidential minutes

Boardmate uses enterprise-grade cloud services and server-side controls rather than improvised document handling. The public summary explains the control model; exact provider names, processing roles, locations, and contractual terms are shared privately during security review.

Managed cloud database infrastructure

Workspace records, review activity, user identity, and audit events are held inside managed cloud database and storage infrastructure designed for production security review.

Secrets stay server-side

Integration secrets and privileged keys are kept out of the browser app. Privileged actions run through server-side functions that verify the caller first.

Access enforced at the data layer

The workspace model is designed around default-deny access, named users, scoped reviewer permissions, and data-layer controls rather than relying only on page-level visibility.

Hardened web delivery

The front end is served over HTTPS with strict transport security (HSTS preload), a content security policy, clickjacking protection (X-Frame-Options: DENY), and MIME-sniffing protection.

The aim is not to hide the detail from serious reviewers. It is to keep exact infrastructure, provider, and integration detail in the private security pack, where it can be reviewed with the right contractual context.

Specialist services, disclosed privately

Boardmate uses specialist services for the jobs that need them: secure hosting, managed database and storage, AI-assisted drafting, enterprise-level voice transcription where recordings are used, monitoring, email delivery, and optional workflow integrations. The public site describes the roles; the private pack identifies the providers.

Core platform	Managed cloud database, authentication, file storage, and server-side execution support the private workspace, source material, drafts, review activity, exports, and audit record.
AI-assisted drafting	Flagship AI capability is used to support drafting and regeneration from supplied meeting material. Customer content is processed to provide the service, not to train public models under the applicable provider terms.
Voice transcription	Enterprise-level voice transcription can convert recordings into source material for minutes where a customer uses recordings in the workflow.
Protection and monitoring	Rate limiting, bot protection, operational monitoring, and diagnostics help keep the service available and secure while avoiding unnecessary exposure of board content.
Communications	Email delivery and public enquiry handling support website enquiries, reviewer notifications, and operational messages.
Optional integrations	Optional meeting import, e-signature, or workflow integrations are used only when enabled for the relevant customer workflow.

The exact subprocessor list, role descriptions, data categories, locations, transfer terms, and data-processing terms are available privately for security and procurement review.

Encryption, access, and identity

How material is protected in transit and at rest, and how access is controlled and recorded.

In transit	All traffic to and from the application is encrypted over HTTPS/TLS; the site enforces HTTPS with HSTS preload so connections cannot silently downgrade.
At rest	Database and file storage are encrypted at rest by managed platform services; customer data sits in production-grade managed infrastructure, not ad-hoc servers.
Authentication	Named users authenticate through managed identity controls. Privileged server functions verify the caller before acting; session and password handling are not hand-rolled.
Authorisation	Default-deny access and scoped permissions mean a user only reaches the records they are entitled to; admin and maintenance operations are separated from ordinary app access.
Reviewer access	External reviewers use scoped, revocable links rather than accounts, and their activity is recorded against the meeting.
Audit record	Access, comments, uploads, decisions, regeneration, and exports are recorded so the history of a meeting's record can be reconstructed.

Data flow, retention, and review

The questions security teams ask first, answered at a level you can act on before requesting the full appendix.

Ingest	Your team uploads a meeting manifest and source material into the scoped workspace. Confidential material should wait until data-handling terms are agreed.
Processing	Boardmate preflights matching, drafts minutes, coordinates review, and regenerates from accepted feedback, within the workspace boundary.
External services	Supporting services are mapped by role, data category, and purpose in the private security pack, so reviewers can inspect the current detail without publishing the operating stack.
Access control	Named workspace users versus scoped reviewer links, with expiry, revocation, and an activity record explaining who saw what, when.
Retention & deletion	Source files, drafts, and final records follow documented retention and deletion controls, agreed in the relevant customer or evaluation terms.
Residency	Data residency requirements can be confirmed before confidential evaluation material is loaded.

Taking it further: this public overview is designed to be useful without giving away the operating stack. Formal commitments are set out in the signed evaluation, subscription, or customer documents. Ask us for the private security pack when your team is ready to review the exact implementation.

Request the private security pack

We can share current data-flow, subprocessor, retention, deletion, access-control, and contractual documentation for your review. **Book a demonstration** at boardmate.app.