

BoardCue Live Security and Information Governance Overview

Last updated: 2 October 2026

Status: Enterprise assurance draft

Current cloud AI processing architecture

BoardCue sends authorised cloud AI requests directly to the Google Gemini Developer API (<https://generativelanguage.googleapis.com>) and OpenAI API (<https://api.openai.com>), using server-held credentials and server-selected models. No Lovable intermediary AI gateway is used in this processing path. The Google service is the Gemini Developer API, not Vertex AI.

Requests using /v1/chat/completions, including product analysis, summaries, minutes, questions, public/support chat and PDF OCR, may make at most 1 alternate-provider attempt when the alternate credential is configured. Failover is permitted for HTTP 401, 402, 403, 404, 429, errors marked retryable by the transport (including HTTP 500 and above, network/read errors, timeouts and unexpected native PDF response-normalisation errors), missing primary credentials or unreadable JSON responses. The original messages, retrieved context and attachments can therefore reach both providers during one logical request; model and provider-specific options are adapted. Input validation, size-limit failures and other non-retryable failures do not trigger failover. This does not guarantee that the alternate provider accepts every payload.

Embeddings do not fail over: product embeddings use Google's gemini-embedding-001 with 3,072 dimensions and response validation. Google PDF OCR sends inline PDF page data to the native generateContent endpoint; it does not upload to a Files API, but remains eligible for chat-path failover. Response parsing after the transport has returned does not itself trigger provider failover. Standard live speech recognition uses the browser/OS speech service, not this cloud AI transport. Local-browser AI is rejected by the server adapter and has no cloud fallback.

The repository establishes API routing, not the supplier account's contractual status. The applicable Google Gemini Developer API and OpenAI API account terms, billing/service tier, DPA and transfer safeguards, processing geography, content-use/training settings, logging and retention must be verified and recorded by the supplier-assurance owner. No zero-retention, UK-only or specific regional AI processing, Google Cloud enterprise controls, enhanced OpenAI retention terms or special contractual arrangement is asserted here.

1. Scope

This document describes the current security and information-governance position without claiming certifications or controls that have not been verified.

2. Data classification and intended use

BoardCue is designed for confidential corporate governance information across sectors. It is not intended to replace sector-specific operational systems or to act as the primary repository for routine individual case-management records. Governance material should use aggregated, anonymised, summarised or otherwise appropriately governed information where practical, while recognising that sensitive workforce, incident, complaint, safeguarding or other case-related information may legitimately appear in board and committee papers.

3. Hosting and data location

The production Supabase project, including its primary database and document storage, is hosted in the United Kingdom. Enterprise deployments are to use Supabase Pro or higher under the current assurance baseline. Supabase publishes automatic daily database backups with the last 7 days available on Pro.

4. Identity, access and MFA

- Authenticated user access through Supabase-backed identity controls.
- Organisation owners/admins can require MFA for organisation users.
- Role and committee access controls restrict governance content by intended membership.
- Row-level database access controls support tenant separation.
- Privileged operations use stronger authentication controls in relevant routes.
- Server-side AAL2 enforcement hardening for all protected organisation operations is an identified assurance improvement.

5. AI security and governance

Cloud AI requests are initiated through authenticated BoardCue server functions and routed through the direct Google Gemini Developer API and OpenAI API services. Provider/model selection is controlled server-side. Exact AI provider processing geography, logging, retention and downstream provider account controls remain subject to written vendor confirmation.

BoardCue is designed to distinguish evidence from AI interpretation and retain human responsibility for governance judgement.

6. Browser transcription

Managed Live Board transcription uses browser/OS speech recognition. The customer organisation is responsible for approving and configuring its endpoint/browser environment. ADEPTABLE does not control or warrant how the third-party browser/OS provider processes speech audio. BoardCue stores the transcript text returned to the application according to the customer's governance lifecycle.

7. Email and attachments

Resend is used for outbound transactional email and Postmark for inbound intelligence email. Inbound attachments enter quarantine and the scanning integration is fail-closed if the required malware scanning configuration is absent. The production malware scanning provider must be verified before being listed as an active subprocessor.

8. Support access

Support access is designed to require explicit customer authorisation, be time-limited, revocable and audited, and be read-only by default. Exceptional write-capable support must use additional controls and be necessary to resolve the relevant issue.

9. Deletion and exit

The revised exit design provides a full organisation export, a 14-day read-only download window and deterministic deletion. This is an implementation gate and should not be represented as fully operational until engineering verification is complete.

10. Incident management

ADEPTABLE's processor breach-notification rule is awareness-based: notification without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, with a 24-hour operational target where practicable. Initial notification can be followed by phased updates.

11. Current assurance status

Cyber Essentials

Status: Not currently claimed. Planned assurance programme item.

Independent penetration test

Status: Not currently claimed. Required before large-scale enterprise rollout.

ISO 27001 / SOC 2

Status: Not claimed by ADEPTABLE. Supplier certifications may be referenced only as supplier evidence.

Sector-specific assurance

Status: Not treated as evidence that BoardCue processes individual case records. Maintain supplier-position statement and complete if a customer/procurement requires it.

Sector-specific technology assurance

Status: Maintain readiness mapping where relevant; not represented as a universal product certification.

Sector-specific safety standard

Status: Current governance intended use is provisionally outside operational case-management Health IT scope; reassess if product use changes materially.

Availability SLA

Status: 99.5% draft target only. Do not activate contractually until health monitoring can calculate monthly Core Platform Availability.