

BoardCue Live Data Retention and Deletion Schedule

Version: 30 August 2026

Status: Revised draft aligned to intended exit workflow

1. Principles

- Customer-controlled governance records may legitimately be long-lived while the workspace is active.
- Derived AI/search data should not outlive its source without a documented reason.
- Deletion of an individual user must not delete organisation-owned governance records.
- On organisation closure, processor data should be returned/exported or deleted according to customer instruction.
- Protected backups can remain beyond live deletion only until the verified backup cycle expires and must remain beyond normal use.

2. Retention schedule

Data class	Default / target	Trigger	Disposal / notes
Active organisation Customer Content	Customer-controlled while contract/workspace active	Customer deletion or termination	Delete/export under customer instruction; no default age-expiry of active board records.
Derived chunks/search/embeddings	No longer than source	Source deletion	Cascade/delete derived representations.
Transcript text / stored AI outputs	Same as related Customer Content	Source/user deletion or customer retention rule	Delete with related governance record.
Browser/OS speech audio	Not retained by BoardCue as application audio in managed browser route	Speech recognition event	Third-party browser/OS provider processing is governed by customer endpoint choice and provider terms.
Organisation exit archive	14 days after customer notified export is ready, where Full Exit workflow is enabled	Termination/expiry	Read-only download, then delete archive as closure process completes.
Terminated active-system Customer Content	Target completion within 30 days after export window/deletion instruction	End of export window or immediate deletion instruction	Deterministic live-system deletion; retain only narrow controller/legal records.
Supabase protected database backups - enterprise baseline	Ordinary Pro daily-backup cycle, current published access window 7 days	Live deletion / backup expiry	Beyond normal use; deletion state reapplied if restored. Verify actual plan/settings at go-live.
Security/audit records	12 months default unless part of customer governance record or active investigation	Event date	Rolling deletion/anonymisation, with extension for legal hold/investigation.
Contracts/billing/legal records	6 years after end/relevant accounting period unless law requires longer	Contract/accounting close	Secure archive then deletion.
Incident/complaint records	6 years after closure unless legal hold	Case closure	Minimise to evidence necessary for accountability.

3. Full Organisation Exit workflow

1. Workspace becomes read-only on the effective termination date.
2. BoardCue generates a complete organisation export for authorised organisation administrators.
3. Customer is notified when the export is ready; the download window lasts 14 calendar days where this workflow is enabled.
4. Customer can request immediate deletion instead of using the export window.
5. At the end of the window, automated deletion of active Customer Content and derived data begins.
6. Deletion should complete within 30 days of the window closing, subject to verified service-specific mechanics.
7. Protected backup copies expire through the ordinary provider cycle and are not restored to ordinary use without reapplying the deletion state.
8. A deletion completion record is retained as narrow accountability evidence.

4. Implementation gate

The 14-day workflow should be made unconditional in public terms only after the Full Organisation Exit Export, read-only closure state, complete database/storage deletion cascade and automated tests have been implemented and verified for the relevant deployment.