

Security Addendum

Technical and organisational measures in place for the Quorval platform — including the measures that are not in place.

Status. This addendum describes the technical and organisational measures actually in place on the effective date, and names the measures that are not. It is referenced by section 3 of the Quorval DPA. Nothing here is a certification or a third-party attestation.

1. Access control and identity

- Authentication through the managed auth service with email/password, Google and Apple sign-in. No anonymous sign-up.
- Multi-factor authentication is enforced for privileged platform and vendor-support roles.
- Roles are stored in a dedicated table, never on the user or profile record, and are evaluated through a security-definer function to prevent privilege escalation.
- Organization admins can force a password reset on next login; invited users set their own credentials through a tokenised link.
- Authentication events, including IP address and user agent, are written to an audit log.

2. Tenant isolation

Quorval runs a shared multi-tenant PostgreSQL database. Every public-schema table has row-level security enabled with explicit grants, and policies are scoped by organization membership. A deterministic monthly probe checks every tenant-scoped table for enabled RLS, policy coverage, absence of blanket-read policies and organization scoping inside shared retrieval functions; the most recent run passed 212 of 212 checks and results are retained as evidence. Cross-tenant access exists only for audited vendor support gated by an organization toggle, and for signed, revocable stakeholder links scoped to one project.

3. Encryption

- TLS 1.2 or better enforced for customer traffic, backend calls, edge functions and sub-processor calls.
- AES-256 at rest on the managed database cluster and object storage, with provider-managed keys.
- Application-layer encryption (pgcrypto) for stored secrets and portal access tokens.
- Secrets held in the platform secret store; never in source control or the browser bundle.

Not available. Customer-managed encryption keys (CMEK/BYOK) are not offered. If your policy mandates CMEK, Quorval does not meet it today.

4. Storage authorization

Every bucket holding customer content is private. Read and write access is scoped to the owning project or organization and checked by a security-definer function rather than a blanket authenticated-user rule.

Branding assets are stored under an organization-keyed path. Anonymous read access to customer content buckets has been removed.

5. Application security

- Input sanitisation with DOMPurify on rendered rich content; no unsanitised HTML rendering in customer-facing views.
- Edge functions verify JWTs manually and derive the caller identity from validated claims.
- Webhook payloads (meeting bot) are verified with HMAC-SHA256 signatures.
- Dependency scanning is run on the codebase; the spreadsheet library with known advisories has been removed in favour of a hardened alternative.
- Recurring automations are instrumented with a job runner and watchdog so silent failure is detected.

6. AI-specific controls

- An internal AI system registry records each model use, its purpose and its human-in-the-loop checkpoint.
- A scheduled evaluation harness scores tenant isolation, citation integrity, extraction precision and coach grounding. Current results: isolation 100%, citation integrity 90%, extraction precision 86%, coach grounding 77%.
- Model outputs are presented as drafts for human review and are attributed as AI-generated in the artifact record.
- No customer data is used for model training by Quorval or its model providers on the contracted tier.

Honest limitation. Coach grounding at 77% means roughly one in four sampled coach responses did not fully ground its claims in retrieved source material. That is a live gap, it is tracked, and we publish it rather than reporting only the numbers that flatter us.

7. Logging, monitoring and retention

Record type	Retention	Notes
Customer content	For the subscription term, then deleted within 30 days of the export window closing	Controller-configurable deletion within the product
Encrypted backups	Provider cycle, currently up to 35 days	Rolling; deletion completes when the cycle expires
Authentication and audit events	24 months	Immutable; retained for security investigation and legal defensibility
E-signature evidence	As required by the customer's own record-keeping obligation	Cryptographically bound to the signed artifact
Meeting recordings and transcripts	Customer-controlled; deleted with the parent project	Sub-processor copies subject to Recall.ai retention terms

8. Operational and organisational measures

- A control register with scheduled evidence collection operates on a monthly and quarterly cadence.
- Change management through version-controlled deployments with the ability to revert.
- Personnel are bound by confidentiality; access to production is limited to the minimum required roles.
- Incident response follows the Vulnerability Disclosure Policy timelines and the 48-hour breach notification commitment in the DPA.

9. Measures we do not yet have

- No independent penetration test. Scoped, not commissioned. This is our most significant open gap.
- No SOC 2 report, ISO 27001 or ISO 42001 certificate, and no external readiness assessment.
- No tested disaster recovery exercise; we rely on provider backups and have not rehearsed a full restore.
- No data residency selection or dedicated single-tenant instance.
- No 24/7 staffed security operations centre; alerting is automated and response is business hours plus best effort.
- No paid bug bounty programme.

Security contact: **security@quorval.com**. Vulnerability reports are handled under the published Vulnerability Disclosure Policy.