

SECURITY CONTROLS

PROOF Technical and Organisational Measures

The current control framework for identity, data protection, governed AI and security operations.

PROCUREMENT DOCUMENT

Version 1.1 | 20 September 2026 | proofhq.io/trust

The current signed agreement controls where it differs from this document.

Technical and organisational measures for the PROOF service.

These measures describe the current control design. Customer-specific commitments and any negotiated requirements are recorded in the signed DPA and order documents.

Domain	Measure	Implementation
Access control	Least privilege and named access	Database roles, scoped permissions, MFA and managed credentials
Tenant isolation	Organisation separation	PostgreSQL row-level security and tenant-scoped application context
AI authority	No autonomous write to customer truth	Governed approval and publisher pathways
Encryption	Protection in transit and at rest	TLS in transit and managed platform encryption for stored data
Change control	Versioned and verified production change	Source control, migrations, automated checks and served verification
Logging	Security and reliability metadata	Technical logs designed to exclude evidence bodies and brief content

People and machines receive only the authority they need.

PROOF separates end-user permissions, administrative access, service roles and AI components.

User identity Authenticated users operate inside an organisation and assigned role.	Database enforcement Protected records remain subject to row-level security regardless of interface behaviour.
Administrative access Named, minimal, MFA-protected and used only for support, maintenance, incidents or law.	Machine identity Service roles are scoped by function. AI and agents cannot bypass the governed write boundary.
Secrets Production credentials are held in managed environment stores rather than source code.	Access review Roles and privileged paths are reviewed as part of governed release and operational work.

Data is minimised, attributed and recoverable.

PROOF's purpose requires a durable evidence record, but the platform limits passive collection and separates technical operations from customer content.

Control	Current measure
Data minimisation	No passive mailbox or calendar access, call recording or background listening in the current product.
Attribution	Material evidence retains person, source, date and governed status.
Retention	Purpose-bound by data class; contractual export and deletion on termination.
Backups	Daily backup and point-in-time recovery capability, retained in-region.
Environment separation	Production and non-production organisations are distinct; demos use synthetic data.
Audit engagements	Working data is destroyed after findings are produced; the report and integrity record remain.

Controls are supported by operating procedures.

PROOF treats incidents, provider changes, recovery and customer requests as governed operational work.

Incident response Assessment, containment, customer notification, recovery and corrective action.	Vulnerability handling Reports are received at security@proofhq.io and triaged against affected services.
Provider governance The production-derived sub-processor register is versioned and material changes are notified.	Recovery Managed backup capabilities support restoration; published CRM state remains in the customer system.
Personnel confidentiality People with production access are subject to confidentiality obligations.	Customer assurance DPA, TOMs, provider information and security questionnaires are supplied during procurement.

Assurance status

PROOF does not yet hold SOC 2 or ISO 27001 certification. Certification remains on the roadmap; this document does not imply otherwise.