CONSTRUCTIONS PILOT

Security Overview

Platform controls, data protection & compliance posture

Version **2026.04** · Generated **June 11, 2026**
Constructions Pilot Pty Ltd · ABN 87 366 101 186
Contact: **security@constructionspilot.com**

PUBLIC — NO NDA REQUIRED

1. About this document

This Security Overview summarises the technical, organisational and contractual safeguards Constructions Pilot operates to protect customer data on the Constructions Pilot platform (the "Platform"). It is intended for the security, procurement and legal teams of customers and prospects evaluating the Platform.

A more detailed SOC 2 Type II report and our Data Processing Agreement (DPA) are available under a mutual non-disclosure agreement — request via **security@constructionspilot.com** or the public Trust Centre at **https://constructionspilot.com.au/trust**.

2. About Constructions Pilot

Legal entity	Constructions Pilot Pty Ltd
Registered jurisdiction	Australia (Victoria)
ABN	87 366 101 186
Product	Cloud SaaS — construction project management, BOQ, procurement
Customers	Construction estimators, project managers, builders & suppliers
Security contact	security@constructionspilot.com

3. Hosting & infrastructure

Primary hosting region	United States (primary) (Replit cloud platform)
Compute	Container-based, isolated workloads, automated horizontal scaling
Database	Managed PostgreSQL with daily backups + WAL streaming
Object storage	Encrypted at rest (AES-256), per-tenant logical separation
Edge / CDN	Cloudflare-fronted reverse proxy with WAF and DDoS protection
DNS	DNSSEC-aware authoritative DNS with redundant providers

4. Encryption

In transit	TLS 1.2 / 1.3 enforced for all customer-facing traffic, modern cipher suites only, HSTS on all production domains

At rest	AES-256 across managed Postgres, object storage and all encrypted backups
Secrets	Stored in the platform secret store. No secrets in source control. CI secret scanning on every commit.
Customer-managed keys	Not currently offered — see roadmap section

5. Authentication & access control

End-user authentication	Federated (Google Sign-in, Replit) and email/password
Password storage	Werkzeug PBKDF2 password hashing with per-user salt; bcrypt-grade strength
MFA / 2FA	TOTP available to all users; **enforced** for admin accounts
Session management	Server-side sessions, rotating IDs, signed cookies, configurable timeout
Authorisation	Role-based: User, Company Member, Company Owner, Admin. Tier-based feature access.
Privileged access	Admin actions logged immutably (Security Audit Log model). Access reviewed quarterly.

6. Data protection & privacy

Tenancy model

Logical multi-tenancy at the database level — every project, BOQ item, file and PO carries an owner / company foreign key, enforced by application-layer checks on every read and write.

Privacy framework

- **Australian Privacy Act 1988** — APP 1–13 mapped, Notifiable Data Breaches Scheme honoured (72-hour regulator notice).
- **GDPR (EU)** — lawful basis recorded, EU SCCs in place for sub-processors, self-service DPA via Privacy Centre.
- **ePrivacy** — granular cookie consent banner, withdraw any time.

Data subject rights (response SLAs)

Access & export	Self-service from Privacy Centre. Verified requests fulfilled within 30 days.
Correction	Self-service for most fields; assisted via support otherwise (≤ 14 days).
Deletion	Verified requests fulfilled within 30 days, audit-logged.

Restriction / objection	Granular consent toggles in Privacy Centre.

7. Backup, resilience & disaster recovery

Backup cadence	Daily full + continuous WAL streaming (Postgres)
Backup retention	30 days rolling, encrypted, off-region
RPO target (contractual SLA)	≤ 24 hours (effective < 15 min via WAL streaming)
RTO target (contractual SLA)	≤ 8 business hours
DR drill	Quarterly restore-to-staging exercise; results captured in evidence vault
Public health endpoint	https://constructionspilot.com.au/trust/health (DB, cache, worker)

8. Monitoring, logging & incident response

- Structured application logs centralised and searchable; retention aligned with retention policy table.
- Suspicious activity alerting: failed-login bursts, IP velocity, privilege escalation, abnormal export volume.
- Error capture (Sentry-class) with PII scrubbing on the producer side.
- Incident response playbook reviewed annually (latest review available in evidence vault).
- Customer notification within 72 hours of confirmed breach per APP NDB Scheme & GDPR Art. 33.
- Coordinated disclosure: vulnerability reports to **security@constructionspilot.com** acknowledged within one business day.

9. Vulnerability management & secure development

Dependency audit	Continuous in CI; critical/high CVEs blocked from merge
SAST	Static analysis on every change
Secret scanning	Pre-commit + CI
Penetration testing	Annual third-party engagement; ad-hoc scans on major releases
Code review	Mandatory peer review + automated checks before merge to production branch
Change management	All production changes via version control with audit trail (immutable git history). Reversible deploys.

10. Sub-processors & vendor management

We use a minimal set of vetted sub-processors. Each holds an independent attestation (SOC 2 Type II or ISO 27001) and a signed DPA with us. The current list is published at **https://constructionspilot.com.au/trust** and updated whenever a vendor changes; existing customers are notified at least 30 days before any new sub-processor is added.

11. Compliance roadmap

Framework	Status
SOC 2 Type II	In progress — auditor engaged, evidence collection underway. Type II observation period commenced 2026 Q1.
ISO 27001	Planned — not before SOC 2 attestation closes
GDPR (EU)	Compliant — DPA + EU SCCs in place
Australian Privacy Act 1988 / NDB Scheme	Compliant
PCI DSS	Out of scope — payment processing fully delegated to Stripe (PCI DSS Level 1)

12. People & security training

- Confidentiality & acceptable-use commitments signed at onboarding.
- Annual security awareness training; new joiners trained within 30 days.
- Production access granted on a need-to-know basis; reviewed quarterly.
- Off-boarding checklist removes access within 24 hours of separation.

> This document is provided for informational purposes only and does not constitute a binding contractual commitment. Specific contractual terms, including service levels, are governed by the Master Services Agreement and the Data Processing Agreement signed between Constructions Pilot Pty Ltd and the customer. For the latest version of this Security Overview and the current sub-processor list, visit **https://constructionspilot.com.au/trust**.