TRUST & COMPLIANCE

RILLA Shield

Procurement Trust Pack

Generated: 24 Aug 2026
Version: 1.0
security@rillashield.app

PACK CONTENTS

HOW TO USE THIS PACK

This document is for procurement, vendor-risk, insurer and auditor review. It consolidates the public compliance information available at rillashield.app/trust. A counter-signable DPA and full evidence under NDA are available on request from security@rillashield.app.

IMPORTANT DISCLAIMER

This pack describes security controls and compliance activities that RILLA Shield Defence currently operates. It is not a SOC 2 audit report, ISO 27001 certificate, or any other formal attestation. SOC 2 Type 1 is targeted for Q4 2026 and will be issued by an independent licensed CPA firm. No certification is claimed that we do not hold.

SECURITY & CONTROLS SUMMARY

Data residency

Australia (ap-southeast-2, Sydney)

Encryption

TLS 1.2+ in transit · AES-256 at rest

Authentication

Password + TOTP MFA · SAML SSO on Business

Access control

RBAC (Owner / Admin / Approver / Viewer) + RLS on every table

Audit log

Immutable, append-only, 12-month retention

Network

Cloudflare WAF + DDoS · no public database

Backups

Daily encrypted · 7-day point-in-time recovery

AI handling

Stateless, de-identified · no third-party model training

SUB-PROCESSORS

RILLA engages the following sub-processors to deliver the Service. All operate under written DPAs and are notified of material changes with 30 days' notice. No customer data is sold or used to train third-party models.

Supabase
- Purpose: Database, auth, storage
- Region: AU (ap-southeast-2)

Cloudflare
- Purpose: Edge delivery, DNS, DDoS
- Region: Global edge; AU termination

Stripe
- Purpose: Subscription billing
- Region: AU / global; PCI DSS Level 1

Resend
- Purpose: Transactional email
- Region: US / EU

Twilio
- Purpose: SMS approvals
- Region: Global

Lovable AI Gateway
- Purpose: Risk reasoning (no retention)
- Region: Gateway-managed

Basiq
- Purpose: Bank account verification
- Region: AU

DATA PROCESSING ADDENDUM (TEMPLATE)

Customer is the Data Controller. RILLA is the Data Processor.

Processing subject matter: detection and prevention of invoice fraud, payee verification, supplier risk scoring, and production of evidence packs in the event of a suspected incident.

Data subjects: customer's employees, suppliers, and counterparties referenced in invoices and payment instructions.

Personal Data categories: business contact details, banking identifiers (BSB / account / IBAN), ABN/ACN, email metadata, invoice contents.

Security measures: TLS 1.2+ in transit, AES-256 at rest, Row Level Security on all customer data, immutable audit log, MFA available to all users, Australian-region hosting.

Breach notification: RILLA notifies the customer without undue delay and within 72 hours of becoming aware of a Personal Data breach affecting customer data.

Retention and deletion: on termination, customer data is deleted within 30 days unless retention is required by law.

Sub-processors: see the Sub-processors section above. Material changes notified with 30 days' notice.

A counter-signable version is available on request from security@rillashield.app.

PENETRATION TEST SUMMARY

Latest internal red-team review: complete. No critical or high-severity findings open. All medium findings remediated prior to release.

Scope: public web application, authenticated user surface, server functions, public /api endpoints.

Method: authenticated and unauthenticated testing against a production-equivalent environment. OWASP Top 10 coverage plus business-logic abuse scenarios specific to invoice fraud (payee tampering, approval bypass, evidence-pack manipulation).

Independent third-party penetration test: scheduled. Full report available under NDA on completion.

SOC 2 & CERTIFICATION ROADMAP

RILLA Shield Defence is preparing for a formal SOC 2 Type 1 examination. The roadmap below is current as of this document's generation date.

Internal readiness pack	Jun 2026	Complete
Continuous monitoring platform	Jul 2026	Complete (Vanta)
Auditor engaged (Type 1)	Aug 2026	Engaged
Observation window	Sep 2026	In progress
SOC 2 Type 1 report issued	Q4 2026	Targeted
SOC 2 Type 2 report issued	Q3 2027	Targeted
ISO 27001 certification	2027	Roadmap

CONTACT

Security and compliance questions: security@rillashield.app

Procurement and vendor onboarding: partners@rillashield.app

Public trust pages: rillashield.app/trust · rillashield.app/trust-center

APPENDIX A

SOC 2 Type 1 Readiness Pack

The following pages contain the complete RILLA Shield SOC 2 Type 1 Readiness Pack, including control mapping against the AICPA Trust Service Criteria (Security, Availability & Confidentiality).

This appendix is a self-assessment and is not a SOC 2 audit report. A formal SOC 2 Type 1 report can only be issued by an independent licensed CPA firm after a formal examination.

SOC 2 Type 1 Readiness Pack

Control mapping against the AICPA Trust Service Criteria — Security, Availability & Confidentiality.

Entity	RILLA Shield Defence Pty Ltd (in formation)
Service	RILLA Shield — AI-powered invoice & payee fraud defence
Audit framework	AICPA SOC 2 Type 1 (Trust Service Criteria, 2017)
Scope	Production web application, server functions, database & supporting infrastructure
Status	Readiness — controls in place; formal audit target Q1 2027
Document version	v1.0 — June 2026
Owner	Security & Engineering, RILLA Shield Defence

1 · Executive summary

This pack maps RILLA Shield Defence's current security, availability and confidentiality controls to the AICPA Trust Service Criteria used in a SOC 2 Type 1 audit. It is intended for prospective auditors, insurer procurement teams and enterprise customers reviewing RILLA prior to engagement.

What this document is: a self-assessed readiness review describing controls in operation today. **What this document is not:** a SOC 2 audit report — that can only be issued by a licensed CPA firm after a formal Type 1 examination. RILLA's target audit window is **Q1 2027**, with a Big-4-adjacent auditor (shortlist: Prescient Assurance, Johanson Group, Sensiba).

Snapshot

Trust Service Criterion	Coverage	Status
CC — Common Criteria (Security)	61 / 64 sub-criteria	**Ready**
A — Availability	Full	**Ready**
C — Confidentiality	Full	**Ready**
PI — Processing Integrity	Not in scope	**Out of scope**
P — Privacy	Partial — APP-aligned	**Roadmap (Type 2)**

2 · System description

Service offered

RILLA Shield is a cloud SaaS that scans invoices, supplier emails and payee bank details to detect business email compromise (BEC), invoice fraud and scam payment instructions before funds leave the customer's account. The platform is delivered via web application, browser extension, email forwarding inbox and authenticated API.

Architecture

Layer	Component	Provider / region
Edge / runtime	Cloudflare Workers (TanStack Start SSR + server functions)	Cloudflare — global edge, AU PoPs
Data store	PostgreSQL with Row-Level Security on every table	Supabase — Sydney (ap-southeast-2)
Authentication	Supabase Auth — JWT, MFA-capable, HIBP password screening	Supabase — AU
AI inference	Lovable AI Gateway (no customer data retained by model providers)	Gateway-managed
Object storage	Encrypted buckets, signed URLs only	Supabase Storage — AU
Email/SMS	Resend (transactional), Twilio (SMS approvals)	US / global, TLS in transit
Payments	Stripe — PCI-DSS Level 1; no card data touches RILLA	Stripe AU
Monitoring	Cloudflare logs, Supabase audit log, internal alerting	AU + global

Data classification

Class	Examples	Handling
Restricted	BSB / account numbers, ABN, supplier banking changes	AES-256 at rest, TLS 1.2+ in transit, RLS-scoped
Confidential	Invoices, email contents, supplier records	Customer-scoped via RLS, deleted on request
Internal	Audit logs, scan metadata	12-month retention, immutable
Public	Marketing pages, /trust content	No restriction

3 · Trust Service Criteria — control mapping

The following sections map RILLA Shield Defence's controls to the AICPA Trust Service Criteria. Each control is in operation today; evidence will be provided to the auditor under NDA.

CC1 — Control environment

Ref	Criterion	RILLA control in operation
CC1.1	**Integrity & ethical values**	Code of Conduct; founder-signed acceptable-use policy; supplier background checks before production access.
CC1.2	**Board oversight**	Founder + advisory board review security posture quarterly; minuted.
CC1.3	**Organisational structure**	Documented org chart; segregation between engineering, support and finance roles.
CC1.4	**Commitment to competence**	Annual security awareness training; phishing simulation; onboarding checklist.
CC1.5	**Accountability**	Named control owners per TSC; performance reviewed quarterly.

CC2 — Communication & information

Ref	Criterion	RILLA control in operation
CC2.1	**Internal information quality**	Centralised runbooks, ADRs, incident retros in shared workspace.
CC2.2	**Internal communication**	Slack security channel; weekly security stand-up; status page.
CC2.3	**External communication**	/trust, /trust-center, /security pages; security@rillashield.app monitored 24h; status.rillashield.app.

CC3 — Risk assessment

Ref	Criterion	RILLA control in operation
CC3.1	**Objectives specified**	Documented security objectives mapped to TSC; reviewed annually.
CC3.2	**Risks identified**	Risk register updated quarterly; threat-modelling on major releases.
CC3.3	**Fraud risk**	BEC, insider-misuse, supplier-impersonation modelled — RILLA's own product mitigates these for customers.
CC3.4	**Change assessment**	Pre-deployment risk review for changes affecting authentication, RLS or payment flows.

CC4 — Monitoring activities

Ref	Criterion	RILLA control in operation
CC4.1	**Ongoing evaluation**	Daily automated dependency scans; weekly RLS policy review; monthly access review.
CC4.2	**Deficiency communication**	Findings tracked in issue system with SLA: critical < 24h, high < 7d, medium < 30d.

CC5 — Control activities

Ref	Criterion	RILLA control in operation
CC5.1	**Selection of controls**	Controls selected against AICPA TSC and OWASP ASVS L2.
CC5.2	**Technology controls**	Branch protection; mandatory code review; CI gates for linter + dependency scan; secret scanning.
CC5.3	**Policies & procedures**	Information security policy, access control policy, incident response plan, vendor management — version-controlled.

CC6 — Logical & physical access controls

Ref	Criterion	RILLA control in operation
CC6.1	**Logical access — restricted**	Supabase Auth + JWT; MFA available to all users; HIBP breached-password screening enabled; role-based access (Owner/Admin/Approver/Viewer).
CC6.2	**User registration**	Email verification mandatory; admin invitations for team seats; no anonymous sign-up to paid tiers.
CC6.3	**Access modification**	Self-service password reset via PKCE token; admin-initiated role changes logged to immutable audit_log.
CC6.4	**Physical access**	No RILLA-owned data centres. Cloudflare + Supabase SOC 2 Type 2 reports cover physical security (sub-processors).
CC6.5	**Logical separation**	Row-Level Security enforced on every public-schema table; tenant_id scoping verified by automated test suite.
CC6.6	**Boundary protection**	Cloudflare WAF + DDoS; rate limiting on auth and scan endpoints; bot management.
CC6.7	**Restricted data in transit**	TLS 1.2+ enforced; HSTS preload; no plaintext fallbacks.
CC6.8	**Malicious software**	Sandboxed file parsing; signed evidence packs; no user-uploaded code execution paths.

CC7 — System operations

Ref	Criterion	RILLA control in operation
CC7.1	**Detection of anomalies**	Cloudflare analytics + Supabase audit log + custom anomaly alerts on failed-auth bursts, RLS denials, payout-changes.
CC7.2	**Monitoring**	24/7 uptime monitor; on-call rotation; PagerDuty-equivalent escalation.
CC7.3	**Incident response**	Documented IR runbook; 72-hour customer notification commitment for breaches affecting customer data.
CC7.4	**Incident handling**	Post-incident retro mandatory; root-cause + corrective action recorded.

Ref	Criterion	RILLA control in operation
CC7.5	**Recovery**	Daily encrypted backups; PITR up to 7 days; cross-region restore tested quarterly.

CC8 — Change management

Ref	Criterion	RILLA control in operation
CC8.1	**Authorised changes**	All production changes via reviewed pull request; protected main branch; signed migrations; rollback plan required.

CC9 — Risk mitigation

Ref	Criterion	RILLA control in operation
CC9.1	**Business disruption mitigation**	BCP/DR plan; quarterly restore test; multi-region read replicas (roadmap).
CC9.2	**Vendor & business partners**	Sub-processor list maintained at /compliance/sub-processors; DPAs in place; annual vendor review.

A — Availability

Ref	Criterion	RILLA control in operation
A1.1	**Capacity planning**	Edge runtime auto-scales; database tier sized for 20× current peak; capacity reviewed monthly.
A1.2	**Backups & recovery**	Daily encrypted backups; PITR 7 days; quarterly restore drill — last drill: passed.
A1.3	**Recovery testing**	Documented RTO 4h / RPO 1h for production database.

C — Confidentiality

Ref	Criterion	RILLA control in operation
C1.1	**Identification of confidential data**	Data classification policy; restricted fields tagged at schema level.
C1.2	**Disposal**	Customer-initiated deletion within 30 days of termination; cryptographic erasure of backups on retention expiry.

4 · Sub-processors

RILLA Shield uses the following sub-processors. All sub-processors are bound by data-processing agreements and (where applicable) Standard Contractual Clauses. Customers are notified of material changes with 30 days' notice.

Sub-processor	Purpose	Region	Certifications
Cloudflare, Inc.	Edge runtime, WAF, DDoS protection	Global edge (AU PoPs)	SOC 2 Type 2, ISO 27001, PCI-DSS
Supabase Inc.	Database, auth, storage	Sydney (ap-southeast-2)	SOC 2 Type 2, HIPAA-eligible
Stripe Payments Australia	Subscription billing	Australia	PCI-DSS Level 1, SOC 1/2
Resend	Transactional email	US / EU	SOC 2 Type 2
Twilio	SMS approvals	Global	SOC 2 Type 2, ISO 27001
Lovable AI Gateway	Model inference (no retention)	Gateway-managed	Zero-retention model providers

5 · Audit roadmap

Milestone	Target	Status
Internal readiness pack (this document)	Jun 2026	**Complete**
Continuous monitoring platform (Vanta / Drata) selected	Jul 2026	**In progress**
Auditor engaged (Type 1)	Aug 2026	**Shortlist drafted**
Observation window opens	Sep 2026	**Pending**
SOC 2 Type 1 report issued	Q1 2027	**Targeted**
SOC 2 Type 2 observation window (6 months)	Q1–Q3 2027	**Targeted**
SOC 2 Type 2 report issued	Q4 2027	**Targeted**

6 · Contact

Security: security@rillashield.app
Procurement / vendor onboarding: partners@rillashield.app
Status page: status.rillashield.app
Public trust pages: rillashield.app/trust · rillashield.app/trust-center · rillashield.app/trust/soc2

Disclaimer. This Readiness Pack is a self-assessment prepared by RILLA Shield Defence. It is not a SOC 2 audit report and does not constitute an attestation under AT-C section 105 or 205. A formal SOC 2 Type 1 report will be issued by an independent licensed CPA firm following the audit window noted in section 5. This pack is made available to prospective auditors, insurers and enterprise customers for procurement-review purposes only.