SOC 2 Readiness Summary

Public overview of PasskeyBridge's SOC 2 readiness, control coverage, and supporting evidence available under NDA.

DOCUMENT	SOC 2 Readiness Summary v1.4
ISSUED	September 29, 2026
STATUS	Readiness only • No audit firm engaged • No audit scheduled
CRITERIA	Security, Availability, Confidentiality (TSC 2017, with 2022 points of focus)
AUDIENCE	Enterprise prospects, procurement, vendor security review teams

1. Programme status

PasskeyBridge's SOC 2 work covers the Security, Availability, and Confidentiality trust services criteria and is readiness only: control mapping, evidence automation, and policy documentation. No audit firm is engaged yet and no audit is scheduled; we are evaluating audit firms. ISO 27001 is the same: readiness only, with no audit firm engaged and no audit scheduled.

2. Trust services criteria coverage

Criterion	Status	Evidence stream
CC1 Control Environment	Mapped	Security policy and contribution rules in the repository; a formal org chart and role register are not yet documented
CC2 Communication & Information	Mapped	Trust Center, status page, changelog, evidence-request pipeline
CC3 Risk Assessment	Mapped	Quarterly access reviews, weekly penetration-test output; no standalone risk register yet
CC4 Monitoring Activities	Operational	Daily codebase sweep, anomaly scanner, canary mesh, function-status metrics
CC5 Control Activities	Operational	Branch ruleset requiring a pull request and passing CI, SHA-pinned Actions, pre-commit secret scan
CC6 Logical & Physical Access	Operational	Multi-tier admin gate, has_role check, breakglass M-of-N, RLS audit
CC7 System Operations	Operational	Live monitoring workflow, status snapshots, canary alerts; incident register deployed, not yet exercised
CC8 Change Management	Operational	PR-based deploys, ci.yml gates, bundle/secret/edge checks
CC9 Risk Mitigation	In progress	Sub-processor list with 30-day change notice; DPAs, cyber-insurance and vendor-risk review in progress
A1 Availability	Operational	/status snapshots, uptime SLOs
C1 Confidentiality	Operational	Zero-PII at edge, AES-256-GCM PBPBV, BLAST tunnels, BYOK

3. Evidence available under NDA

Enterprise prospects executing a mutual NDA receive the full readiness package, which includes:

- Control matrix mapping every TSC criterion to the implementing code, configuration, or runbook.
- CI hardening evidence: ci.yml, live-monitoring.yml and daily-sweep.yml workflow definitions and recent run logs.
- Output of the weekly internal penetration-test suite: anonymous reads and writes against row-level security, authentication fuzzing of edge functions, sensitive-column exposure, cross-tenant reads, admin-scope escalation, and secret configuration checks.
- Breakglass session logs demonstrating M-of-N approval, time-bounded access, and append-only audit trail.
- DSAR cadence: tombstoning erasure with the affected row count read back per table, and a sample fulfilment timeline.
- Vendor sub-processor list and the Schrems III hashed-signal architecture diagram. Executed sub-processor DPAs are in progress and not yet part of the package.
- Incident response playbooks and 72-hour breach notification runbook (GDPR Article 33).
- Daily codebase sweep aggregating secrets/PII/RLS/dist/bundle/edge/audit/memory checks.

4. Architectural commitments backing the controls

- **Zero-PII at the edge.** Phone numbers and other primary identifiers are hashed with keyed HMAC-SHA-256 under a server-held pepper at the ingestion boundary, and the plaintext is never stored or logged. A phone number leaves the platform only for a carrier lookup a tenant requests, to that lookup's provider; the Privacy Policy (section 10) lists what each sub-processor receives.
- **Tenant isolation.** Every multi-tenant table enforces row-level security keyed on tenant_id, so a dashboard session reads only its own organization's rows. Edge functions run with a service role that bypasses row-level security; each authenticates the tenant first and scopes every query to it in code.
- **Bring Your Own Key (BYOK).** A tenant can import its own EC P-256 or P-384 signing key for credentials and attestations; otherwise the platform generates one.
- **DSAR erasure.** Erasure runs the DSAR tombstoning path: identifier columns nulled and encrypted columns overwritten, scoped by tenant and keyed digest, with the audit row kept.
- **Append-only audit trails.** Breakglass actions, admin mutations, and DSAR erasure events are written to the audit log, which no client can update or delete.
- **Hybrid post-quantum signatures.** ML-DSA-65 (NIST FIPS 204) co-signs identity assertions alongside classical ECDSA.

5. Out of scope for this summary

This public summary intentionally does not include: specific control failure remediations, internal infrastructure diagrams, vendor pricing, or anything that could materially aid an attacker. Those artefacts are covered by the full readiness package made available under a mutual NDA.

6. Requesting the full readiness package

Submit a request at passkeybridge.io/security/soc2-request with your work email, company, and intended use. Our security team replies within one business day with the NDA and the full evidence package. Direct contact: security@passkeybridge.io.

PasskeyBridge LLC. This document describes our current readiness posture and is not a SOC 2 attestation report. No audit firm is engaged and no audit is scheduled.