SOC 2 Readiness Summary

Version: 2026-04 · **Owner:** Engineering · **Distributed as:** `Votriz_SOC2_Readiness.pdf`

Status

Votriz is **SOC 2 aligned**. We do not yet hold formal Type I attestation; the audit window opens **Q4 2026** with Type II following six months later in **Q2 2027**. This document maps the Trust Service Criteria to controls already running in production so auditors and procurement teams can evaluate readiness today.

Trust Service Criteria coverage

CC1 — Control environment

- AI Safety Officer designated (Founder/CTO, contact security@votriz.com).
- Code of conduct and AI principles documented in `AI_GOVERNANCE_POLICY.md`.
- Engineering changes go through `pre_prod_validation.sh` — multi-tenant isolation regressions block merges.

CC2 — Communication & information

- Compliance Center page (votriz.com/compliance) is the canonical customer-facing surface.
- Status page (`votriz.com/status`) for runtime availability.
- Internal incident response procedures: `AI_INCIDENT_RESPONSE.md`.

CC3 — Risk assessment

- AI model inventory + risk classification: `AI_MODEL_INVENTORY.md`.
- Vendor risk assessment template (pre-completed): `VENDOR_RISK_ASSESSMENT.md`.
- Sub-processor list maintained in `DATA_PROCESSING_AGREEMENT.md` with 30-day customer notice on changes.

CC4 — Monitoring activities

- `daily_metrics.sh` — operational health snapshot run by the on-call engineer.
- `GET /audit/log/summary` — queryable activity rollup for owners and admins.
- Resend webhook + post-metrics-sync cron — SLA monitoring for the email + social pipelines.

CC5 — Control activities

- Five-role RBAC enforced via `services/permissions.py`'s `require_permission()` dependency on every mutating route.
- Brand-level scoping via `users_brand_access`.
- Per-user permission overrides via `user_permission_overrides`.

CC6 — Logical & physical access

- JWT (HS256, 15-minute access + 30-day refresh; secrets in hardware-backed secure storage).
- Application-level `org_id` derivation on every request — never client-supplied.
- PostgreSQL Row-Level Security policies on all nine tenant-scoped tables (deployed; activation Q4 2026 when the application connection role moves off `votriz` superuser).
- Operator access only via an encrypted VPN tunnel — no port-forwarded shell access on the public internet.
- AES-256 at rest (Fernet-wrapped OAuth tokens; volume-level encryption for the database tier).

CC7 — System operations

- Deployment via an automated pipeline — diff-able, reversible, no manual production-host steps.
- `scripts/disaster_recovery.sh` documents the full recovery procedure; restore drill runs monthly.
- Runtime metrics shipped to Prometheus via the `ObservabilityMiddleware`.

CC8 — Change management

- Every deployable change goes through git — atomic commits visible in `git log`.
- Pre-prod validation blocks merges that regress multi-tenant isolation.
- Database migrations in `db/migrations/NNN_*.sql` are versioned and applied in order; rollback procedure documented in `SECURITY_ARCHITECTURE.md`.

CC9 — Risk mitigation

- Vendor risk assessment process covered by `VENDOR_RISK_ASSESSMENT.md`.
- Multi-provider AI fallback (Anthropic → OpenAI) so a single provider outage doesn't degrade the platform.
- Backup + restore-drill cadence documented in `DATA_RETENTION_POLICY.md`.

Honest gaps before formal attestation

These will close before the Q4 2026 audit window:

1. **RLS activation** — policies are deployed but the connection role bypasses them. Move to a non-superuser role and set `app.current_org_id` in the per-request middleware. Tracked in the `SECURITY_ARCHITECTURE.md` roadmap.
2. **Third-party penetration test** — scheduled Q3 2026.
3. **MFA enrollment for owner / admin roles** — TOTP flow implementation lands in this sprint; mandatory enforcement becomes a contract requirement for Enterprise tier.
4. **Automated retention jobs** — the policy is documented, but archival of `audit_log`, `email_sends`, `analytics_snapshots`, `form_submissions`, and `tag_history` past their stated windows currently requires a manual run. Auto-archive cron lands in Q3.
5. **Vendor attestation collection** — periodic re-collection of sub-processor SOC 2 reports / equivalents currently happens at contract renewal; will move to quarterly under the formal process.

What auditors should look at first

Concern	Where to look	Endpoint / file
Tenant isolation evidence	Live runtime + pre-deploy gate	`GET /security/isolation-proof` + `scripts/pre_prod_validation.sh`
Audit log immutability	Database trigger	`\d security_audit_log` → `no_audit_update` trigger
Access control enforcement	Live route gating	`services/permissions.py` + `require_permission` decoration grep
Encryption posture	Documented + live	`SECURITY_ARCHITECTURE.md` §2
Sub-processor list	DPA appendix	`DATA_PROCESSING_AGREEMENT.md` §3
AI risk inventory	Inventory doc	`AI_MODEL_INVENTORY.md`
Incident response	Playbook	`AI_INCIDENT_RESPONSE.md`

Roadmap

- 2026-Q3: third-party pen test + automated retention jobs
- 2026-Q4: SOC 2 Type I audit window opens; RLS activation
- 2027-Q2: SOC 2 Type II attestation
- 2027: ISO 27001 + ISO 42001 (AI management systems)