

Security & Operational Trust

Built for regulated, high-availability estates

SynapseTel Cloud engineers, modernizes and operates critical telecom and enterprise cloud infrastructure. Our engagements involve core network elements, hybrid data centers and production CI/CD pipelines. Security governs how we access your environment, how we write and ship code, and how we control automated workflows.

v7.0 · Policy updated: October 19, 2026

Contracting entity	Registration	Jurisdiction
SYNAPSETEL CLOUD LLC	L26000459009	Florida, United States

1. Client-boundary execution & zero production-data custody

Boundary isolation is our primary engagement control. Proprietary data, network topologies and source code remain inside your approved security perimeter.

In-boundary engineering

Assessment, migration and implementation work runs in your designated cloud accounts/VPCs, on-premises VMware/vSAN estate or Red Hat OpenShift clusters. Engineers connect through your approved bastion hosts, VDI or Zero Trust Network Access (ZTNA) gateways.

No production-data exfiltration

We do not copy, store or process Customer Proprietary Network Information (CPNI), subscriber PII, production databases or live network packet captures on SynapseTel-owned infrastructure.

Controlled artifact handling

Architecture diagrams, dependency graphs and runbooks remain in client-controlled repositories and document stores. Any non-production diagnostic metadata explicitly authorized for local analysis is encrypted and deleted at engagement completion under the agreed secure-deletion procedure, using cryptographic erasure where supported.

This boundary applies to production engineering material. Our separate administrative portal processes permitted contact, account, service and billing records; its handling is described below.

2. Identity, access & change governance

Engineering access uses your identity provider (IdP), Privileged Access Management (PAM) workflows and named accounts. Access remains subject to your approval, review and revocation.

Least privilege and just-in-time access

We scope roles to the approved task and support just-in-time privilege elevation. SSH, Kubernetes API and cloud-console session recording is configured through your supported access and logging controls.

Hardware-backed authentication

Our engineering endpoint standard requires phishing-resistant, hardware-backed MFA using FIDO2/WebAuthn, together with cryptographic SSH authentication and signed code changes. Customer access follows the authentication mechanisms supported and approved by your IdP and PAM systems.

GitOps production change control

Routine production changes follow a signed-code, peer-review and policy-validation workflow. Merge/pull requests identify the change and approvals; GitLab CI runs validation, and a GitOps controller such as Argo CD reconciles approved declarative configuration. Network-element changes use the customer-approved automation and change-control path.

Ad-hoc production changes are prohibited. Emergency intervention follows the customer’s authorized break-glass procedure, with session evidence, retrospective review and reconciliation into the source of truth.

3. Infrastructure, Kubernetes & telecom hardening

Our engineering baseline covers workload isolation, management-plane segmentation, software provenance and secret delivery. The design records the controls applicable to each supported workload and any approved exception.

Domain	Engineering standard
Kubernetes & OpenShift	Target restricted security profiles, including OpenShift restricted-v2 SCCs where applicable, non-root execution, seccomp RuntimeDefault and dropped Linux capabilities (ALL). Configure read-only root filesystems separately and validate the effective SCC and namespace permissions at admission.
Network segmentation	Default-deny ingress and egress NetworkPolicies, explicit allowed flows, and mTLS where the selected services support it. Separate OSS/ENM management planes, CAMARA/NEF/SCEF API adapters, gateways and public-facing portals with approved firewall zones.
Supply chain & CI/CD	Verify image provenance, generate software bills of materials (SBOMs), scan vulnerabilities and apply agreed CVE thresholds before registry promotion. Use OPA Gatekeeper or Kyverno admission policies where selected for the target platform.
Secrets management	Keep plaintext secrets out of Git. Deliver credentials, certificates and API tokens through approved enterprise secret managers such as HashiCorp Vault, or through appropriately configured External Secrets or Sealed Secrets workflows.

SCC admission, a read-only root filesystem, network encryption and supply-chain gates are distinct controls. Vendor-supported CNFs or other workloads requiring an exception need documented security review and compensating controls.

4. AI agents & Model Context Protocol guardrails

AI-assisted delivery and custom MCP integrations operate within explicit data, tool and approval boundaries.

Private, approved model execution

Customer workflows use enterprise-approved private inference endpoints, such as self-hosted OpenShift AI or vLLM models running inside your security boundary. Proprietary code, manifests and telemetry are excluded from public consumer AI services. Model-provider retention and no-training terms must be approved before use.

Deterministic tool scoping

MCP servers expose explicit read-only or schema-restricted tools with scoped service accounts. Agents cannot invoke arbitrary shells or bypass source-system RBAC. The connected service enforces authorization for each action.

Human approval for production changes

Agents can prepare manifests, run pre-flight checks and assemble control evidence. Production mutations require an authenticated, attributable human approval and deterministic CI/CD validation; signing and approval evidence are bound to the proposed change.

Customer-retained audit trails

Prompts, context retrievals and MCP tool invocations generate audit records in your central SIEM or observability stack. Log content, redaction, access and tamper-resistant retention are configured within your boundary to protect secrets and sensitive context.

A passing pre-flight report does not authorize deployment or establish rollout health. Target-system authorization, admission controls and operational acceptance remain in force.

5. Regulatory & compliance alignment

We map engineering controls and delivery evidence to the obligations and control sets selected for your engagement. Applicability, evidence requirements and acceptance owners are recorded with your security team.

Enterprise security frameworks

Control mapping for SOC 2 Type II criteria, ISO/IEC 27001 and NIST SP 800-53 Rev. 5.

Telecom & critical infrastructure

Relevant 3GPP Security Assurance Specifications (SCAS), FCC CPNI obligations and NIS2 requirements, as applicable to your services and jurisdiction.

Cloud & container benchmarks

Applicable CIS Benchmarks for Kubernetes and Red Hat OpenShift, with workload exceptions and remediation evidence documented.

Control alignment and generated evidence do not establish certification or guarantee regulatory compliance. SynapseTel Cloud has not undergone a SOC 2 Type I or Type II examination. Upstream provider reports cover the providers' own services.

6. Internal endpoint security & personnel

Personnel and endpoint requirements apply before engineers receive access to client systems.

US-based principal engineering

Engagements are led by vetted senior principal architects operating from the United States. Delivery responsibilities and authorized personnel are identified for the engagement.

Hardened workstations

Corporate engineering devices require full-disk encryption using FileVault or BitLocker, automated patch management, endpoint detection and response (EDR), and enforced firewall policies.

Confidentiality first

We execute a mutual non-disclosure agreement before architecture discovery or repository review. Client material is handled through the approved access and confidentiality boundaries.

Customer-specific screening, residency, device posture and access evidence are addressed during onboarding.

7. Security contact & vulnerability disclosure

Client InfoSec and procurement teams can request questionnaire responses and engagement-specific evidence. Researchers can report potential vulnerabilities in synapsetel.com or our public assets through the same security contact.

Security email

security@synapsetel.com

Acknowledgement

We acknowledge security inquiries and vulnerability reports within 24 hours.

Include the affected URL, a concise description, reproduction steps and your contact details. Avoid subscriber data, credentials or destructive testing. Coordinate any testing beyond normal use with us in advance.

[View our security.txt disclosure contact](#)

Administrative portal & assurance boundary

The zero-production-data-custody model does not eliminate administrative processing. Our portal uses Netlify for hosting, Supabase for authentication, database and private files, Stripe for billing, and GitHub for application source control.

Permitted administrative records

The portal processes identities, authorized contacts, service requests and status, approved documents, agreements and billing references. Production configurations, raw diagnostics, secrets and subscriber records stay in customer-controlled systems.

Application access and files

Portal access combines authenticated identities, organization membership, role checks and database/storage policies. Staff access requires two-step verification. Private document delivery checks record access before issuing a short-lived signed URL.

Evidence and continuity

Application checks and provider assurance are distinct from an independent organizational audit. Attachment validation does not establish automated DLP or malware scanning. Customer production runtimes remain independent of the portal; the engagement records alternate coordination and incident-notification routes.

The engagement agreement records permitted processing, retention and deletion, incident obligations, access controls and service responsibilities. Website inquiry acknowledgement is separate from contracted operational response and resolution targets.

Provider assurance references

Review the covered product, audit period, plan and report-access terms directly with each provider.

[GitHub](#)

[Netlify](#)

[Supabase](#)

[Stripe](#)