

Sécurité et confiance opérationnelle

Pour les environnements réglementés et à haute disponibilité

SynapseTel Cloud conçoit, modernise et exploite des infrastructures critiques télécom et cloud d'entreprise. Nos missions concernent des éléments de cœur de réseau, des datacenters hybrides et des pipelines CI/CD de production. La sécurité régit nos accès, le développement et la livraison du code et le contrôle des processus automatisés.

v7.0 · Politique mise à jour: 19 octobre 2026

Entité contractante	Immatriculation	Juridiction
SYNAPSETEL CLOUD LLC	L26000459009	Florida, United States

1. Exécution dans le périmètre client et absence de garde des données de production

L'isolation des périmètres est notre principal contrôle de prestation. Données propriétaires, topologies et code source restent dans votre périmètre de sécurité approuvé.

Ingénierie dans votre environnement

Évaluation, migration et réalisation s'exécutent dans vos comptes/VPC cloud, votre infrastructure VMware/vSAN sur site ou vos clusters Red Hat OpenShift. Les ingénieurs passent par vos bastions, VDI ou passerelles ZTNA approuvés.

Aucune exfiltration de données de production

Nous ne copions, ne stockons ni ne traitons CPNI, données personnelles d'abonnés, bases de production ou captures de paquets en direct sur une infrastructure appartenant à SynapseTel.

Gestion contrôlée des artefacts

Schémas, graphes de dépendances et procédures restent dans les dépôts et espaces documentaires du client. Toute métadonnée de diagnostic hors production expressément autorisée pour analyse locale est chiffrée puis supprimée en fin de mission selon la procédure convenue, par effacement cryptographique lorsque possible.

Cette limite concerne les éléments techniques de production. Le portail administratif distinct traite les contacts, comptes, services et données de facturation autorisés, décrits plus bas.

2. Identité, accès et gouvernance des changements

L'accès technique utilise votre IdP, vos processus PAM et des comptes nominatifs. Vous conservez l'approbation, la revue et la révocation des accès.

Moindre privilège et accès temporaire

Les rôles sont limités à la tâche approuvée et peuvent bénéficier d'une élévation just-in-time. L'enregistrement SSH, API Kubernetes et consoles cloud est configuré avec vos dispositifs d'accès et de journalisation compatibles.

Authentification matérielle

Notre standard des postes d'ingénierie impose une MFA matérielle résistante au phishing avec FIDO2/WebAuthn, l'authentification SSH cryptographique et la signature des changements de code. Les accès client suivent les mécanismes compatibles et approuvés de votre IdP et PAM.

Contrôle GitOps de la production

Les changements courants suivent code signé, revue par les pairs et validation de politiques. Les merge/pull requests identifient changement et approbations ; GitLab CI valide et un contrôleur GitOps comme Argo CD réconcilie la configuration déclarative approuvée. Les éléments réseau suivent l’automatisation et le contrôle des changements autorisés par le client.

Les modifications improvisées en production sont interdites. Une urgence suit la procédure break-glass autorisée du client, avec traces de session, revue rétrospective et réconciliation avec la source de vérité.

3. Durcissement infrastructure, Kubernetes et télécom

Le socle couvre isolation des charges, segmentation de gestion, provenance logicielle et fourniture de secrets. La conception consigne les contrôles de chaque charge prise en charge et les exceptions approuvées.

Domaine	Standard d’ingénierie
Kubernetes et OpenShift	Profils restreints, dont SCC restricted-v2 d’OpenShift lorsque pertinent, exécution non root, seccomp RuntimeDefault et suppression des capacités Linux (ALL). Configurer séparément la racine en lecture seule et valider SCC effectif et droits du namespace à l’admission.
Segmentation réseau	NetworkPolicies refusant par défaut entrées et sorties, flux explicitement autorisés et mTLS lorsque les services le permettent. Zones de pare-feu séparant gestion OSS/ENM, adaptateurs CAMARA/NEF/SCEF, passerelles et portails publics.
Chaîne d’approvisionnement et CI/CD	Vérifier la provenance des images, générer les SBOM, analyser les vulnérabilités et appliquer les seuils CVE convenus avant promotion. Politiques d’admission OPA Gatekeeper ou Kyverno si retenues pour la plateforme cible.
Gestion des secrets	Aucun secret en clair dans Git. Fournir identifiants, certificats et jetons par les gestionnaires approuvés, tels que HashiCorp Vault, ou des processus External Secrets ou Sealed Secrets correctement configurés.

Admission SCC, racine en lecture seule, chiffrement réseau et contrôles logiciels sont distincts. Les CNF ou charges exigeant une exception nécessitent une revue documentée et des contrôles compensatoires.

4. Agents IA et garde-fous Model Context Protocol

La livraison assistée par IA et les intégrations MCP respectent des limites explicites de données, outils et approbations.

Exécution privée et approuvée des modèles

Les processus client utilisent des points d’inférence privés approuvés : des modèles OpenShift AI ou vLLM auto-hébergés dans votre périmètre. Code, manifestes et télémétrie propriétaires sont exclus des services IA grand public. Les conditions de rétention et de non-entraînement doivent être approuvées avant usage.

Outils déterministes et délimités

Les serveurs MCP exposent des outils en lecture seule ou limités par schéma avec comptes dédiés restreints. Les agents ne peuvent lancer de shell arbitraire ni contourner RBAC. Le service connecté autorise chaque action.

Approbation humaine en production

Les agents peuvent préparer manifestes, prévalidations et preuves de contrôle. Les mutations exigent une approbation humaine authentifiée et attribuable et une validation CI/CD déterministe ; signature et approbation sont liées au changement.

Traces conservées par le client

Prompts, recherches de contexte et invocations MCP produisent des traces dans votre SIEM ou observabilité centrale. Contenu, masquage, accès et rétention résistante aux altérations sont configurés dans votre périmètre pour protéger secrets et contexte sensible.

Une prévalidation réussie n'autorise pas un déploiement et n'établit pas sa santé. Autorisation du système cible, admission et réception opérationnelle restent applicables.

5. Alignement réglementaire et conformité

Nous relient contrôles et preuves aux obligations et référentiels retenus pour la mission. Applicabilité, preuves requises et responsables de réception sont documentés avec votre équipe sécurité.

Référentiels de sécurité entreprise

Correspondance avec critères SOC 2 Type II, ISO/IEC 27001 et NIST SP 800-53 Rev. 5.

Télécom et infrastructures critiques

Spécifications SCAS 3GPP, obligations FCC CPNI et exigences NIS2 pertinentes selon vos services et votre juridiction.

Référentiels cloud et conteneurs

CIS Benchmarks applicables à Kubernetes et Red Hat OpenShift, avec exceptions et preuves de remédiation documentées.

L'alignement et les preuves ne constituent pas une certification et ne garantissent pas la conformité. SynapseTel Cloud n'a pas fait l'objet d'un examen SOC 2 Type I ou Type II. Les rapports fournisseurs couvrent leurs propres services.

6. Sécurité des postes et personnel

Les exigences de personnel et de poste s'appliquent avant l'accès aux systèmes client.

Direction technique depuis les États-Unis

Les missions sont dirigées par des architectes principaux seniors évalués opérant depuis les États-Unis. Responsabilités et personnel autorisé sont identifiés pour la mission.

Postes durcis

Les postes d'ingénierie d'entreprise exigent chiffrement intégral FileVault ou BitLocker, gestion automatisée des correctifs, EDR et politiques de pare-feu appliquées.

Confidentialité dès le départ

Un accord mutuel de confidentialité est signé avant découverte d'architecture ou revue des dépôts. Les éléments client suivent les périmètres d'accès et de confidentialité approuvés.

L'intégration traite vérifications, résidence, posture des appareils et preuves d'accès spécifiques au client.

7. Contact sécurité et divulgation de vulnérabilités

InfoSec et achats peuvent demander questionnaires et preuves propres à la mission. Les chercheurs peuvent signaler des vulnérabilités potentielles de synapsetel.com ou de nos actifs publics au même contact.

Courriel sécurité

security@synapsetel.com

Accusé de réception

Nous accusons réception des demandes de sécurité et signalements de vulnérabilités sous 24 heures.

Indiquez URL affectée, description concise, étapes de reproduction et coordonnées. Évitez données d'abonnés, identifiants et tests destructifs. Convenez préalablement de tout test dépassant l'usage normal.

[Voir le contact de divulgation dans security.txt](#)

Portail administratif et périmètre d'assurance

L'absence de garde des données de production n'élimine pas le traitement administratif. Le portail utilise Netlify pour l'hébergement, Supabase pour authentification, base et fichiers privés, Stripe pour facturation et GitHub pour le code.

Données administratives autorisées

Le portail traite identités, contacts autorisés, demandes et états, documents approuvés, accords et références de facturation. Configurations de production, diagnostics bruts, secrets et données d'abonnés restent sous contrôle client.

Accès applicatif et fichiers

L'accès combine authentification, appartenance à l'organisation, rôles et politiques de base et stockage. Le personnel doit utiliser deux étapes de vérification. La remise privée vérifie l'accès avant une URL signée de courte durée.

Preuves et continuité

Vérifications applicatives et assurance fournisseurs sont distinctes d'un audit organisationnel indépendant. Valider un fichier ne constitue ni DLP automatique ni analyse antimalware. La production client reste indépendante du portail ; la mission consigne coordination alternative et notifications d'incident.

Le contrat consigne traitement autorisé, rétention et suppression, incidents, accès et responsabilités. L'accusé de réception web est distinct des objectifs opérationnels contractuels de réponse et résolution.

Références d'assurance fournisseurs

Vérifiez produit couvert, période, offre et conditions d'accès au rapport auprès de chaque fournisseur.

[GitHub](#)

[Netlify](#)

[Supabase](#)

[Stripe](#)