



MUTUAL NON-DISCLOSURE AGREEMENT (NDA)

Document Reference: STC-NDA-2026-_____ Effective Date: _____

Party A ("SynapseTel")	Party B ("Company")
Legal Entity: SYNAPSETEL CLOUD LLC, a Florida limited liability company Operations Base: State of Florida, United States Notice Contact (Name, Title, Email): _____	Legal Entity: _____ Principal Address: _____ Notice Contact (Name, Title, Email): _____

This Mutual Non-Disclosure Agreement (the "**Agreement**") is entered into as of the Effective Date between **SYNAPSETEL CLOUD LLC** ("SynapseTel") and **Company** (each a "**Party**" and collectively the "**Parties**").

1. Purpose

The Parties wish to explore and potentially execute a technical and commercial relationship relating to telecom management systems (Ericsson OSS-RC / ENM), hybrid cloud and container platforms (Red Hat OpenShift / Kubernetes / VMware vSAN / KubeVirt), DevSecOps and private MCP pipeline automation, portal/API engineering (CAMARA / NEF / SCEF), or an associated **Assessment Sprint** or **Statement of Work ("SOW")** (collectively, the "**Purpose**"). In connection with the Purpose, each Party (as a "**Disclosing Party**") may disclose Confidential Information to the other Party (as a "**Receiving Party**").

2. Definition of Confidential Information

"**Confidential Information**" means any non-public technical, operational, security or business information disclosed by or on behalf of a Disclosing Party to the Receiving Party, whether orally, visually or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure.

- **Company Confidential Information** includes, without limitation: network topologies, node inventories, cmedit/AMOS parameter exports, OpenShift cluster configurations, VMware storage policies, CI/CD logs, security vulnerabilities, audit findings, source code and operational telemetry.
- **SynapseTel Confidential Information** includes, without limitation: non-public reference architectures (.nmd), migration playbooks, schema-restricted MCP tool definitions, security control matrices, commercial pricing proposals and SOW templates.
- **Exclusions:** Confidential Information does not include information that the Receiving Party can demonstrate by written record: (a) is or becomes publicly available through no breach of this Agreement; (b) was rightfully known to the Receiving Party without restriction before disclosure; (c) is rightfully received from a third party without breach of any confidentiality obligation; or (d) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

3. Obligations, Perimeter Security & Private AI Covenant

The Receiving Party shall:

1. **Standard of Care & Need-to-Know:** protect the Disclosing Party's Confidential Information with at least the degree of care it uses for its own confidential information of similar sensitivity (and never less than reasonable care), and restrict access to its employees, principal engineers, contractors and professional advisors who need to know it for the Purpose and are bound by written confidentiality obligations no less protective than this Agreement.
2. **Use Restriction & No Reverse Engineering:** use the Disclosing Party's Confidential Information solely for the Purpose, and not reverse-engineer, decompile or disassemble any software, scripts or prototypes disclosed under this Agreement.
3. **No External AI / LLM Use or Training:** neither Party shall upload, transmit or input the other Party's Confidential Information into any public or third-party external large language model (LLM) or generative AI service, or use it to train, fine-tune or improve any external AI model. Any AI or Model Context Protocol (MCP) pre-flight tooling used during an engagement must run within Company's designated security perimeter on approved, self-hosted endpoints.
4. **No Production Credential Custody:** SynapseTel does not require or retain custody of persistent production credentials, TLS private keys, or subscriber PII/CPNI outside Company's designated bastion/VPN perimeter.

4. Compelled Disclosure

If the Receiving Party is legally compelled by a court, telecom regulator or governmental authority to disclose any Confidential Information, it shall (to the extent legally permitted) give the Disclosing Party prompt written notice so it may seek a protective order or other remedy, and shall disclose only the portion legally required.

5. Return, Destruction & Diagnostic Hygiene

Upon the Disclosing Party's written request, or within ten (10) business days after discussions end without an active SOW, the Receiving Party shall promptly return or destroy all copies of the Disclosing Party's Confidential Information in its possession and, on request, certify the destruction in writing. The Receiving Party may retain (a) deliverables purchased and owned by Company under an executed SOW and (b) routine encrypted system backups or redacted compliance audit logs required by law, which remain subject to this Agreement for as long as they are retained.

6. Ownership & No Implied License

All Confidential Information remains the sole and exclusive property of the Disclosing Party. Nothing in this Agreement grants any patent, copyright, trademark, trade secret or other intellectual property license or right, by implication or otherwise, or obligates either Party to enter into any further agreement or SOW unless separately executed in writing. Confidential Information is provided "AS IS", without warranty of any kind, during pre-SOW evaluation.

7. Term & Survival

This Agreement covers disclosures made from the Effective Date for **two (2) years** or until the expiration of any active SOW between the Parties, whichever is later (the "**Disclosure Period**"). Either Party may end the Disclosure Period early on thirty (30) days' written notice, but not while an SOW between the Parties is active. Ending the Disclosure Period does not release either Party from its obligations for Confidential Information already received: those obligations survive for **three (3) years** from the date of each disclosure and, for trade secrets (including non-public network security architecture), for as long as the information remains a trade secret under applicable law. Sections 2 through 6 and 8 survive any termination of this Agreement.

8. Remedies, Governing Law & General Provisions

1. **Injunctive Relief:** a breach of this Agreement may cause irreparable harm for which monetary damages alone would be inadequate, and the Disclosing Party may seek immediate injunctive or equitable relief in addition to any other remedy available at law.
2. **Governing Law & Venue:** this Agreement is governed by the laws of the **State of Florida, United States of America**, without regard to conflict-of-law principles. Any action arising out of or relating to this Agreement shall be brought exclusively in the state courts located in **Broward County, Florida**, or the United States District Court for the Southern District of Florida. Each Party irrevocably submits to the personal jurisdiction of those courts and waives any objection to venue there, except that either Party may seek injunctive relief under Section 8.1 in any court of competent jurisdiction.
3. **Entire Agreement & E-Signatures:** this Agreement is the entire agreement between the Parties regarding confidentiality before an SOW; once an SOW is executed, it operates alongside that SOW's security provisions. Amendments must be in writing and signed by both Parties. Electronic signatures and PDF counterparts have the same legal effect as original signatures.

IN WITNESS WHEREOF, the Parties have executed this Mutual Non-Disclosure Agreement by their duly authorized representatives as of the Effective Date.

For SYNAPSETEL CLOUD LLC	For Company (legal entity named above)
_____ Signature Printed Name: _____ Title: Founder & Principal Architect Date: _____	_____ Signature Printed Name: _____ Title: _____ Date: _____