

The boundary, the evidence, the roles, the records.

BUILD rc1-6-3 · PREPARED FOR REVIEW UNDER NDA · CONTACT NIGEL@ARQNXS.COM

I.

What the tenant contains, precisely.

Inside the firm's tenant: the application; the model endpoint as an Azure OpenAI resource in the firm's own subscription, referenced by the deployment and never created or held by the vendor; the data VM, carrying the firm's records on its own persistent disk that outlives any redeploy; the gateway that fronts the sealed network; and the firm's Entra directory for identity. The evidence sink, flow-log storage and the log workspace, lives in the tenant too.

Outbound traffic from the sealed network is denied by default. The only application egress the policy allows is the tenant's own model endpoint and Entra for token verification; in the sealed mode that enforcement is always on and cannot be weakened by configuration. Outside the boundary: everything else, including the vendor. The vendor cannot see the firm's trades; that is a property of the architecture, not a contractual promise.

II.

Three artifacts the deployment produces.

EGRESS MANIFEST	Generated from the same registry the runtime enforces, so the document cannot drift from the policy: every network family the server can open, with hosts, purpose, and protocol, per deployment mode. A stale manifest fails the build gate.
FLOW-LOG VERIFICATION	The tenant's own Azure flow logs, classified flow by flow against the manifest: allowed and expected, allowed but unexpected, denied, or infrastructure. The run includes a deliberate denied-egress probe and fails unless that probe shows up denied, because an empty log is not evidence of a sealed box.
PLANE-DENIAL REPORT	A role-by-surface access matrix for a compliance reviewer: which roles reach each oversight surface, what a denied caller receives (a 404, never a 403), and

the structural guarantees that firm-plane routes cannot read trader-plane records. Every row is re-verified live against real routes and a real database on every gate run.

III.

Entra groups map to capabilities.

Entra ID groups map to trader, desk manager, risk, compliance, auditor, and strategy. Officer surfaces are gated by capability, not by convention. Org administration is not oversight: an administrator's rights do not include reading the register.

IV.

The firm's records, under the firm's policy.

Records are append-only and live in the firm's own storage under the firm's retention policy. Every oversight surface prints an audit-stamped PDF on demand: as-of time, generating officer, scope, and the monitoring line naming unmonitored clauses.

DOJIPAD INSTITUTIONAL · ARQNXS OÜ © 2026 · INSTITUTIONAL.DOJIPAD.COM



DojiPad Institutional · ARQNXS OÜ © 2026 · [Privacy](#) · [Terms](#) · [Site notice](#) · [Security disclosure](#) · This site sets no third-party cookies and loads nothing from third-party domains.