SECURITY & ARCHITECTURE

A clear boundary for self-hosted operations.

This planning document summarises the intended deployment model. The final topology and responsibilities are agreed for each customer environment.

CUSTOMER NETWORK
Users and enterprise identity
Reverse proxy / TLS / access policy
Opliora application containers
Customer-controlled PostgreSQL and persistent files
Backups, monitoring and recovery controls

CONTROL AREAS

Security controls by layer

Controls are effective only when technical configuration and operating ownership are both explicit.

Layer	Opliora product	Customer operation
Identity	Role-based access, 2FA support, attributable actions	User lifecycle, directory policy, access review
Application	Controlled releases, migration guidance, audit history	Validation, release scheduling, administrator separation
Data	Application data model and access boundaries	PostgreSQL access, retention, backups, restore tests
Infrastructure	Documented runtime requirements and health endpoints	Hosts, TLS, network, runtime patching, monitoring
Incident	Product triage and remediation within support scope	Detection, containment, evidence, communications, recovery

Evidence required before launch

Use the detailed website runbooks for deployment, access, backup and vulnerability reporting.

CHECK	EVIDENCE / OWNER
Test and production environments are separated	_____
TLS and network exposure are approved	_____
Administrator access uses 2FA	_____
PostgreSQL backup completed and restored successfully	_____
Health checks and alert ownership are confirmed	_____
Rollback decision and named approvers are recorded	_____
Support contacts and severity definitions are agreed	_____
Customer responsibility matrix is signed	_____