SECURITY FRAMEWORK

OMEGANEON LLC

Contents

1. Purpose & Security Principles . . . 3

2. Agent Permission Boundaries (APB) . . . 3

3. Human-in-the-Loop (HITL) . . . 4

4. Execution Security Architecture . . . 4

5. Auditability & Operational Transparency . . . 5

6. Permission Lifecycle Management . . . 5

7. Cloud Deployment & Infrastructure Security . . . 6

7.1 OMEGANEON Hosted Cloud - Default Deployment . . . 6

7.2 Bring Your Own Cloud (BYOC) - Optional Add-on . . . 6

7.3 Restricted Engineer Access & Operational Control . . . 7

7.4 Tenant Isolation & Data Protection . . . 7

8. Security Monitoring & Incident Response . . . 7

9. Customer Control & Shared Responsibilities . . . 8

10. Deployment & Verification . . . 8

11. Contractual Framework . . . 9

Core Commitment . . . 9

OMEGANEON Security Framework

1. Purpose & Security Principles

OMEGANEON's Security Framework governs the authorized execution of AI-powered business workflows across both OMEGANEON Hosted Cloud and customer-owned cloud deployments. Its purpose is to preserve customer control over data and consequential business actions while defining enforceable operational responsibilities.

The framework follows six principles:

1. **Least Privilege:** Agents and service identities receive only the access required for their assigned work.
2. **Default Deny:** Actions lacking valid authorization are blocked.
3. **Human Oversight:** High-impact actions require human approval under the applicable policy.
4. **Enforced Boundaries:** Permission checks occur in execution infrastructure, not solely in AI instructions.
5. **Traceability:** Security-relevant requests, approvals, actions, and changes are recorded.
6. **Revocability:** Authorized administrators can restrict or revoke future access.

Authorization does not imply unrestricted autonomy. The same agent security principles apply to both deployment models.

2. Agent Permission Boundaries (APB)

Every AI agent operates within Agent Permission Boundaries (APB), defined by six **Permission Primitives**. The primitives are authorization dimensions; the values in each dimension are customer- and workflow-specific configurations.

Primitive	Definition
System	Applications, services, environments, or resources an agent may access.
Data	Datasets, records, fields, or information categories an agent may access.
Action	Operations an agent is authorized to perform.
Limit	Quantitative, financial, frequency, volume, and operational constraints.
Duration	The effective period and expiration of the authorization.
Identity	The authenticated identity used and the person or organization represented.

2.1 APB Model

APB = (System, Data, Action, Limit, Duration, Identity)

An operation is authorized only when it satisfies all applicable APB constraints and any required HITL approval. Specific systems, datasets, thresholds, operations, identities, and periods are illustrative configuration values, not additional primitives or exhaustive categories.

Permissions must be explicit, task-limited, enforced at the relevant boundary, verifiable, and revocable. Agents cannot enlarge their own authority; delegated agents cannot exceed the authority available to the delegating workflow.

2.2 Enforcement

Authorization is checked before each protected operation, including tool calls, API requests, and privileged workflow steps. Approval of a workflow does not automatically authorize every subsequent action. Unknown tools, missing permissions, expired authorization, and failed checks result in denial.

3. Human-in-the-Loop (HITL)

HITL specifies when AI may operate autonomously and when human intervention is mandatory.

Level 1 - Autonomous Execution

Authorized, low-risk work can execute automatically within the approved APB. Examples include retrieving permitted data, preparing summaries, and generating internal analyses.

Level 2 - Conditional Execution

Operations with controlled business impact may execute under explicit rules and thresholds. Actions outside those conditions require approval. Examples include authorized record updates, scheduled batches, or communications within an approved policy.

Level 3 - Mandatory Human Approval

High-impact, sensitive, or potentially irreversible operations require explicit human authorization unless prohibited outright. Examples include deleting critical records, initiating payments, changing privileges, or making major production changes. Additional authentication or multiple approvers may be required by policy.

3.1 Approval Requirements

An approval request must identify the proposed action, affected systems and resources, material parameters, expected consequences, requesting identity, applicable APB, approval expiration, and whether the action is reversible.

Approval is bound to the exact operation or expressly defined batch. Material changes require renewed authorization. Rejected, expired, or missing approvals block execution. Agents cannot approve their own restricted actions.

4. Execution Security Architecture

Execution sequence: Agent Request > APB Validation > Risk Classification > HITL Approval (if required) > Controlled Execution > Audit Logging.

4.1 Independent Enforcement

Authorization and execution infrastructure must remain independent of model reasoning. A model may propose an action but cannot override permission checks or approval rules.

4.2 Runtime Controls

- Authenticated customer, operator, and agent identities.
- Tool-, resource-, and environment-level authorization.
- Validation of action parameters and applicable limits.
- Protection against reused approvals and replay attacks.
- Controlled storage and use of service credentials.
- Blocking of unauthorized operations and privilege escalation.

External content, including emails, documents, retrieved webpages, and tool output, cannot grant or expand permissions.

4.3 Multi-Agent Workflows

Every delegated operation remains subject to authorization. Delegation cannot create additional privileges; each executing agent remains within its effective APB.

5. Auditability & Operational Transparency

Security-relevant actions and operational changes must generate structured, protected audit records.

5.1 Audit Events

- Permission grants, changes, expiration, and revocation.
- Protected operations requested, allowed, denied, and executed.
- HITL approvals, rejections, and approval expiration.
- Policy violations, execution errors, and relevant outcomes.
- Deployment, infrastructure, identity, and security-configuration changes.

5.2 Audit Record Contents

Applicable records include timestamp, event identifier, customer/workflow identifier, executing and approving identities, affected resource and operation, policy version, authorization result, and execution outcome. Logs must exclude credentials and unnecessary personal information and must resist unauthorized modification or deletion.

5.3 Customer Visibility

Authorized customer administrators receive the permission, approval, and execution visibility established in the service configuration and agreements. Retention, export, and access rights must be documented.

5.4 Development Transparency

During implementation, customer-visible Development Logs record progress, completed work, tests, blockers, and next steps. Development Logs supplement but do not replace security audit logs.

6. Permission Lifecycle Management

Lifecycle: Request > Review > Authorization > Activation > Monitoring > Modification or Revocation.

6.1 Initial Authorization

Before production activation, OMEGANEON and the customer agree on APB settings, approvals, deployment-specific access, and operational rules.

6.2 Permission Changes

Material increases in access, operational limits, or agent autonomy require authorization from the designated customer authority. Neither engineering personnel nor AI agents may unilaterally expand customer-approved permissions.

6.3 Revocation

Authorized administrators must be able to revoke agent permissions or suspend workflows. Revocation blocks subsequent protected operations when enforced; it does not reverse completed external actions.

6.4 Emergency Suspension

Controls must support suspension of workflows, blocking of future protected calls, and revocation of applicable credentials. Partially completed operations must be recorded and assessed before resumption.

7. Cloud Deployment & Infrastructure Security

OMEGANEON offers **Hosted Cloud as the default deployment model** and **Bring Your Own Cloud (BYOC) as an optional add-on**. Both models deliver AI Workflow Implementation and ongoing Managed Operations. HITL, APB, restricted engineer access, and audit requirements apply to both.

Supporting controls address authentication, encryption, credential management, customer isolation, secure development, prompt-injection defenses, monitoring, backup and recovery, incident response, and data retention. Exact technical configurations and service obligations are established by the applicable agreements and verified before production use.

7.1 OMEGANEON Hosted Cloud - Default Deployment

Under the default model, OMEGANEON provisions and manages the cloud infrastructure used to run authorized customer workflows. Customers do not need to supply or administer a cloud account to receive the managed service.

- **Infrastructure and operations:** OMEGANEON manages provisioning, deployment, routine infrastructure administration, monitoring, maintenance, updates, and operational incident handling within the agreed service scope.
- **Customer data:** Customers retain ownership of their business data. OMEGANEON processes it only for the contracted services and authorized integrations, subject to the applicable DPA and AI Addendum.
- **Tenant boundaries:** Each customer must have technically enforced separation of workflow runtime, data stores, service identities, secrets, queues, logs, and backups according to the documented tenancy design.
- **Commercial arrangement:** Hosting and managed-operation charges, usage allocation, limits, and service coverage are defined in the applicable proposal and SOW.
- **Exit and portability:** Customer data export, deletion, retention, transition assistance, and termination responsibilities are defined contractually.

Third-party model APIs and connected business services may receive authorized data as specified in the approved integrations and contractual documents. Hosted Cloud does not, by itself, establish a fixed data residency commitment.

7.2 Bring Your Own Cloud (BYOC) - Optional Add-on

Under BYOC, workflows run in the customer-owned cloud account while OMEGANEON continues to implement, operate, maintain, and manage the agreed infrastructure and workflow services. BYOC is an alternative hosting arrangement, not a one-time installation.

- **Account authority:** The customer retains cloud-account ownership, ultimate administrative authority, and the ability to revoke OMEGANEON access.
- **Managed operations:** OMEGANEON conducts approved deployments, monitoring, maintenance, updates, troubleshooting, and cloud-management activities through the Engineering Platform within the SOW.
- **Scoped access:** Customer-approved service identities and infrastructure roles are limited to the approved resources and activities. Material privilege expansion requires customer approval.
- **Billing and support:** Cloud-provider charges, BYOC implementation and managed-operation fees, support coverage, backup and recovery duties, and escalation rules are specified in the SOW.
- **Revocation:** Revoking delegated operating access can suspend or limit OMEGANEON managed services until a new authorization is established.

BYOC does not relax APB, HITL, engineer-access, or audit controls. Any data transfers to approved model providers and connected services remain subject to contractual and technical safeguards.

7.3 Restricted Engineer Access & Operational Control

For both Hosted Cloud and BYOC, OMEGANEON engineering personnel perform authorized deployments, monitoring, maintenance, troubleshooting, and cloud-management operations **only through the OMEGANEON Engineering Platform**. Operational access does not grant unrestricted access to customer data or production infrastructure.

1. **No direct raw-data access:** Engineers are not granted direct access to customer production databases, raw business records, or production secrets.
2. **Platform-mediated management:** No unrestricted use of cloud consoles, direct SSH, interactive production terminals, or unmanaged administrator credentials.
3. **Controlled changes:** Deployments and infrastructure changes require approved, verifiable artifacts, explicit permissions, and applicable HITL approvals.
4. **Bounded identities:** Service identities are scoped by purpose, resource, operation, and duration; unauthorized privilege escalation is blocked.
5. **Sanitized diagnostics:** Engineering visibility uses approved metrics, redacted logs, and synthetic/test data rather than raw customer data.
6. **Recorded activities:** Deployments, maintenance, configuration changes, approvals, incidents, and outcomes are associated with authenticated operators and timestamps.

Blocking direct database access is insufficient if deployed software can indirectly access or export sensitive information. Release permissions, artifact behavior, runtime identities, and network egress must therefore be constrained and tested.

7.4 Tenant Isolation & Data Protection

Hosted deployments must implement tenant separation throughout the runtime and data-processing stack. BYOC deployments require equivalent controls appropriate to customer-owned infrastructure and the agreed responsibility split.

- Identity, network, runtime, storage, database, queue, secrets, observability, and backup boundaries are defined and tested.
- Encryption in transit and at rest, credential rotation, and access reviews are applied to relevant resources.
- External data transfer destinations and AI/model subprocessors are documented and controlled according to customer authorizations and agreements.
- Retention, deletion, backup, disaster recovery, and offboarding procedures are defined for each deployment model.
- The Engineering Platform remains separated from customer workload data processing through enforceable access, deployment, and egress controls.

8. Security Monitoring & Incident Response

OMEGANEON provides monitoring, operational triage, and incident-response activities for both deployment models within the service coverage and responsibilities established in the SOW.

1. **Detection:** Identify suspicious, abnormal, or unauthorized activity.
2. **Containment:** Suspend affected workflows, restrict permissions, or disable compromised credentials.
3. **Investigation:** Examine approved logs, events, execution history, and impacted resources.
4. **Remediation:** Address the underlying issue and strengthen controls.
5. **Recovery:** Validate applicable controls before resuming affected services.
6. **Notification:** Inform affected customers as required by applicable agreements and law.

Unauthorized operations must fail closed. Service hours, response targets, escalation, recovery, and notification rules are specified in the SOW; neither model alone promises 24/7 coverage.

9. Customer Control & Shared Responsibilities

Customer ownership of business data applies in both models. Cloud-account ownership, infrastructure administration, billing, and revocation mechanisms differ by deployment arrangement.

Control / Responsibility	Hosted Cloud (Default)	BYOC (Optional)
Cloud account & infrastructure	OMEGANEON provisions and manages the cloud environment.	Customer owns cloud account; OMEGANEON receives limited delegated operating access.
Cloud-provider billing	Handled by OMEGANEON; customer charges follow SOW.	Paid by customer, subject to customer provider terms.
Workflow & cloud operations	OMEGANEON manages the agreed infrastructure and workflows.	OMEGANEON manages the agreed customer infrastructure and workflows.
Business data	Owned by customer; processed under DPA / AI Addendum.	Owned by customer; processed in customer environment and approved integrations.
Approvals & APB	Customer authorizes consequential actions and approved business access.	Customer authorizes consequential actions and delegated cloud/business access.
Service exit	Contractual export, deletion, and transition procedures.	Customer can revoke cloud delegation; operational handover follows SOW.

OMEGANEON Responsibilities

- Implement and enforce agreed APB, HITL, restricted engineer access, and audit controls.
- Provision and manage Hosted infrastructure, or manage expressly delegated BYOC resources, according to SOW.
- Maintain authorized operational records, protect service identities, and handle incidents within agreed scope.
- Document deployment-specific security controls, data processing, operational support, and offboarding procedures.

Customer Responsibilities

- Approve connected business systems, authorized data processing, material APB changes, and human approvers.
- Provide accurate business requirements and customer-controlled account/access information where applicable.
- For BYOC, maintain cloud-account ownership, billing arrangements, and authorization of delegated access.
- Review material operating-policy changes and communicate access, business, and escalation requirements.

10. Deployment & Verification

Before production activation, the controls applicable to the selected deployment model must pass documented acceptance checks. Verification must cover both intended access and attempted bypasses.

Common Requirements - Both Models

- APB and HITL enforce allowed, denied, expired, and changed-parameter operations.
- Delegation, operation limits, suspension, revocation, and audit records work as designed.
- Engineers cannot directly retrieve production raw business records, databases, or secrets.
- Platform-only operations, scoped identities, controlled releases, and network-egress restrictions prevent indirect extraction.

- Sanitized diagnostics, event records, incident procedures, and change approvals are verified.

Hosted Cloud Acceptance

- Tenant boundaries isolate customer data, runtime, credentials, logs, queues, storage, and backups.
- Host-level administrative access, backups/recovery, data export/deletion, and third-party data transfers follow documented controls.

BYOC Acceptance

- Delegated cloud-management roles permit agreed operations but block unauthorized resource or privilege access.
- Customer revocation and handover are tested, and the resulting managed-service impact is documented.

Production use requires completion of applicable acceptance criteria and resolution or formal acceptance of remaining identified risks. An unverified security design must not be represented as an implemented control.

11. Contractual Framework

This framework sets out OMEGANEON's intended security requirements for AI authorization, human oversight, Hosted Cloud, optional BYOC, platform-restricted engineering operations, and operational accountability.

Applicable agreements may include:

- **Professional Services Agreement (PSA)** - the general service relationship and allocation of liability.
- **Statement of Work (SOW)** - selected deployment model, workflow scope, managed cloud services, fees, service hours, support levels, maintenance, backup/recovery, escalation, change approvals, and exit duties.
- **Data Processing Agreement (DPA)** - personal-data processing requirements and applicable subprocessor terms.
- **AI Addendum** - AI-specific data usage, model service providers, approvals, and responsibility boundaries.

Hosted Cloud is the default offering; BYOC is an optional add-on priced and scoped through the customer proposal and SOW. The two options share the same baseline controls but have different cloud account, billing, and access arrangements.

Publication of this framework does not by itself establish regulatory certification, external audit attestation, specific regional data residency, or completion of every security control.

Core Commitment

Customer data remains customer-owned. OMEGANEON implements and manages AI workflows by default on OMEGANEON Hosted Cloud, or as an optional add-on in a customer-owned cloud. APB limits agent authority; HITL governs consequential operations; engineers use restricted platform-mediated access; security-relevant activity remains auditable.

OMEGANEON - Controlled AI Execution & Managed Cloud Operations.