PUBLIC POLICY / PILOT + PRODUCTION

AI ACCEPTABLE USE POLICY

Unified public policy • Applies to Paid Pilot and Production PSA/SOW

Version: 1.4 — Unified Public Policy

Issued: November 19, 2026

Contractual Effective Date: For each Customer, when this version is expressly incorporated into an executed Pilot Agreement or Professional Services Agreement, or separately accepted in writing.

Contact: support@omeganeonhq.com

1. Scope and application

This AI Acceptable Use Policy ("AUP") governs how a customer ("Customer") and its authorized users may use AI-enabled workflow services ("AI Services") provided by Omeganeon LLC ("OMEGANEON") under either (a) an executed Paid Pilot Agreement with its Pilot Statement of Work ("Pilot SOW"), or (b) an executed Professional Services Agreement ("PSA") with its production Statement of Work ("Production SOW"). The relevant signed contract, its applicable SOW and incorporated schedules are together the "Agreement". "SOW" in this policy means the applicable Pilot SOW or Production SOW.

This AUP primarily establishes Customer and authorized-user conduct requirements. OMEGANEON's delivery, sandbox or production security implementation, data protection, intellectual-property and commercial obligations are governed by the applicable Agreement, its Security Schedule, the Data Processing Agreement ("DPA") if applicable, and the AI Addendum. This AUP does not expand OMEGANEON's authorized system or data access.

2. Permitted use and Customer responsibilities

Customer and its authorized users may use AI Services for lawful business purposes within the agreed SOW, approved systems and Agent Permission Boundaries ("APB"). For a Pilot, authorized purposes are limited to the agreed controlled-sandbox evaluation; production use is not authorized by a Pilot Agreement. Customer is responsible for lawful instructions and supplied materials, data-use rights, required notices and consents, authorized users and approvers, and permissions for connected systems under its control.

Customer must designate authorized administrators and approvers, safeguard credentials and promptly revoke or adjust access when authorizations end or roles change.

Customer may request expanded systems, data, actions or limits through the agreed approval/change-control procedure. A lawful request for additional permissions is not itself a violation of this AUP. No requested permission takes effect before approval and technical implementation.

3. Prohibited use

Customer and authorized users must not:

- Access, extract, alter or disclose data or systems beyond approved scope, including information of another customer.
- Circumvent APB, identity controls, multi-factor authentication, required Human-in-the-Loop ("HITL") review, usage limits, monitoring or audit logging.
- Introduce malicious code, conduct unauthorized intrusion/security testing, disrupt services, engage in fraud or unlawful discrimination, or otherwise violate applicable law using AI Services.
- Submit data, credentials, prompts, media or materials without the rights and permissions necessary for intended use.
- Use AI Services for regulated or consequential decisions without required human review; conduct real-world production operations during a sandbox-only Pilot.

- Misrepresent AI-generated material as human-created where prohibited by law or the AI Addendum.

These restrictions do not prohibit lawful requests for additional permissions through an approved process.

4. Agent Permission Boundaries and human approval

Every agent action must remain within six APB dimensions: System (where), Data (what), Action (which operation), Limit (bounds), Duration (when) and Identity (whose authority). No user or agent may self-expand these permissions.

HITL is risk-tiered. Approved routine actions may run automatically within established APB. High-risk, destructive, irreversible, financial or externally consequential operations require human approval when designated in the SOW or Security Schedule; legally mandated human review always applies. Sandbox Pilot workflows must not bypass restrictions on production writes or live external actions.

Customer must identify authorized approvers and follow the agreed decision process. OMEGANEON's implementation duties are in the applicable Security Schedule.

5. Customer data, sensitive information and model training

Customer retains its Input rights and legally existing rights in AI Output. Prototype ownership and temporary Pilot evaluation rights, and production Deliverable assignment after payment where applicable, are defined in the relevant Agreement and AI Addendum. This AUP makes no IP assignment.

The standard service scope excludes special-category personal data, health records, banking credentials and comparable high-risk information unless categories, purposes and safeguards are expressly approved in the applicable SOW and DPA. A Pilot uses synthetic or properly anonymized sandbox data by default. Customer must not introduce Customer Personal Data into a Pilot until the parties have activated the necessary DPA and security controls.

Acceptance of this AUP does not authorize OMEGANEON or model vendors to train on Customer Input, Output or Customer Content. Training exceptions require prior express written authorization specifying vendor/model, data, purposes and safeguards. Customer Input, Output and non-public Customer Materials are not authorized for general product improvement or cross-client reuse.

Permitted limited service telemetry, deletion and lawful retention are governed by the applicable Agreement, DPA, AI Addendum and SOW, not this AUP.

6. Deployment and approved third parties

OMEGANEON-Hosted Cloud (default). OMEGANEON operates the hosting environment and service-side model connections within the agreed scope. A Pilot is a controlled sandbox, not production. Customer authorizes necessary connected-system actions and retains authority over its business instructions and approvals.

Bring Your Own Cloud (BYOC; optional add-on). BYOC applies only when expressly selected in the relevant SOW. Customer controls its cloud account and delegates only the access needed for contracted services; a sandbox-only Pilot remains limited to evaluation.

Actual vendors, regions, tenant isolation, credentials and approved subprocessors are specified in the SOW, DPA or related schedules. All pricing, cloud and AI API usage charges and Change Orders are governed by the applicable Pilot Agreement or PSA/SOW; this AUP imposes no separate fees or automatic usage overages.

7. Security requirements and audit records

Customer and authorized users must not bypass or interfere with required security controls and must cooperate with identity checks, approval procedures, access revocation and security investigations.

The applicable Pilot Sandbox Security Schedule or Production Security Schedule, together with the DPA and SOW when applicable, defines OMEGANEON's safeguards, verification gates, audit-log retention, customer access, backup, recovery and deletion duties. A Pilot's sandbox controls do not imply that production requirements have

been satisfied. Contractually required controls must be implemented and verified before the relevant system or data access, and before Production Go-Live where applicable. Merely listing a control is not a claim that it is operational today.

8. Reporting misuse and responding to security risks

Customer must promptly report suspected misuse, unauthorized agent actions, compromised credentials or security concerns to support@omeganeonhq.com and reasonably assist in containment.

Where an action or workflow creates an active security or misuse risk, OMEGANEON may temporarily restrict the affected action or permission only as authorized by the signed Agreement. Such restriction must be properly scoped, no broader than reasonably necessary, and subject to applicable notice and restoration procedures.

This AUP does not authorize seizure, withholding or deletion of Customer data, unrelated service shutdown or override of lawful customer access. Security incident response and notification duties are governed by the Agreement, DPA and Security Schedule.

9. Version control, changes and precedence

This AUP is version 1.4, issued November 19, 2026. For each Customer, only the version expressly incorporated into its executed Agreement or separately accepted in writing applies. OMEGANEON may publish future versions for new engagements; website posting alone does not amend an existing Pilot Agreement or PSA. Material changes require the respective Agreement's written amendment process. Previous accepted policy versions remain applicable unless validly amended and shall be retained for reference.

If provisions conflict, mandatory law and restricted-transfer clauses control to the extent required; the applicable DPA governs personal-data processing; the AI Addendum governs AI-specific rights; and the Pilot Agreement or PSA/SOW governs its own legal, delivery and commercial subjects, subject to express amendments. This AUP creates no new fees, model-training permissions, IP assignments, warranties or indemnities.

Version history: v1.4 is the policy version approved for new engagements beginning November 19, 2026. Previously accepted versions, including v1.3, remain effective for those Customers unless validly amended. Publication on the website is separate from contractual adoption.