# ACCEPTABLE USE POLICY (AUP)

This Acceptable Use Policy ("AUP") sets forth specific prohibitions and requirements for the use of Orion AI Factory's GPU Cloud Services. Capitalized terms have the meanings given in the Master Services Agreement.

**1. PROHIBITED AI PRACTICES (EU AI ACT & GLOBAL STANDARDS)**

Orion Telekom strictly prohibits the use of its infrastructure for AI practices deemed to carry "Unacceptable Risk" under **Article 5 of Regulation (EU) 2024/1689 (EU AI Act)** or that violate fundamental human rights. You may not use the Services of Orion AI Factory to develop, deploy, or operate:

a. **Social Scoring:** AI systems that evaluate or classify natural persons over a period of time based on their social behavior or known/predicted personality characteristics.

b. **Real-Time Biometric Identification:** The use of AI for "real-time" remote biometric identification in publicly accessible spaces for law enforcement purposes, unless explicitly authorized by judicial order provided to Orion Factory.

c. **Subliminal Manipulation:** AI systems deploying subliminal techniques beyond a person's consciousness to materially distort their behavior.

d. **Vulnerable Group Exploitation:** AI systems that exploit vulnerabilities of a specific group of persons due to their age, disability, or social or economic situation.

e. **Biometric Categorization:** Systems that categorize natural persons based on biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.

**2. NVIDIA LICENSE RESTRICTIONS**

The Services of Orion AI Factory utilize NVIDIA hardware (e.g., H100, B200) and software (CUDA, Drivers, NIMs). The Customer agrees NOT to:

a. **Reverse Engineer:** Decompile, disassemble, or reverse engineer NVIDIA Drivers, CUDA, or NVIDIA AI Enterprise software.

b. **License Bypass:** Attempt to bypass the NVIDIA vGPU licensing grid or software locks.

c. **Cryptocurrency Mining:** Use the Services for cryptocurrency mining (Proof-of-Work) or any blockchain validation that is not explicitly authorized in an Enterprise Order Form.

**3. BENCHMARKING AND COMPETITIVE ANALYSIS**

**Strict Prohibition:** The Customer may not perform, publish, or disclose the results of any benchmarking, performance, or competitive analysis of the Services (including throughput, latency, or scalability metrics) to third parties without Orion Telekom's prior written consent.

**4. CONTENT STANDARDS**

If using the Services to generate content, the Customer must not generate, host, or distribute:

a. **CSAM/NCII:** Child Sexual Abuse Material or Non-Consensual Intimate Imagery (Deepfake Pornography).

b. **Disinformation:** Content intended to mislead the public regarding electoral processes, public health, or emergency services.

c. **Hate Speech & Harassment:** Content that promotes violence, incites hatred, or harasses individuals based on protected characteristics.

**5. SECURITY AND NETWORK ABUSE**

The following activities are strictly prohibited:

a. **Network Scanning:** Port scanning, vulnerability scanning, or penetration testing of Orion Factory's internal or external networks without prior written consent.

b. **Malware:** Hosting, distributing, or operating command-and-control servers for malware, botnets, or ransomware.

c. **DDoS:** Launching Denial of Service attacks or operating "Booter/Stresser" services.

d. **IP Spoofing:** Forging TCP-IP packet headers or any part of the header information in an email or a newsgroup posting.

**6. HIGH-RISK USE DISCLAIMER**

The Services are not designed or intended for use in hazardous environments requiring fail-safe performance, including the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Services could lead directly to death, personal injury, or severe physical or environmental damage.

**7. ENFORCEMENT**

Orion telekom reserves the right to monitor resource usage patterns (e.g., power consumption, network flows) to detect AUP violations. Upon detection of a violation, Orion Telekom may:

a. **Suspend:** Immediately suspend the offending Instance or Account.

b. **Terminate:** Terminate the Agreement for cause without refund.

c. **Report:** Report illegal activities (specifically CSAM, Terrorist Content, and Serious Crime) to relevant law enforcement authorities including **Europol** and the **Ministry of Interior**.