UNIKRON ACCEPTABLE USE POLICY (AUP)

Effective Date: 29.10.2025
Governing Document: UNIKRON Master Terms of Service (Master ToS) (Last Updated: 29.10.2025).

Violation of this AUP constitutes a material breach of the Agreement and is grounds for immediate suspension or termination pursuant to Master ToS Article 6.3.

SECTION 1: PROHIBITED REGULATORY & COMMERCIAL MISUSE

The Client shall not use the Services, or permit the Services to be used, in a manner that:

1.1 Misrepresentation of Services: Characterizes, advertises, markets, or otherwise represents to any third party (including but not limited to customers, regulators, or investors) that Nokor GmbH provides Financial Services, acts as a counterparty, provides investment advice, holds assets, or executes transactions. The Client must actively correct any such misrepresentation by its customers or end-users.

1.2 Regulatory Burden: Requires Nokor GmbH to register, be licensed, or otherwise be regulated as a Money Transmitter, Broker, Dealer, Custodian, or Financial Services Provider in any jurisdiction.

1.3 Illegal Activity: Involves or facilitates illegal gambling, money laundering, terrorist financing, pyramid schemes, fraudulent transactions, or any activity prohibited by Swiss, cantonal, or applicable foreign law.

1.4 Resale of Core Access: Rents, leases, sells, or sublicenses access to the Services to any unaffiliated third party without express written consent from Nokor.

1.5 General Legal Compliance: Violates, or causes Nokor to violate, any applicable law, rule, or regulation in any jurisdiction, including but not limited to economic sanctions programs, anti-money laundering laws, and export control regulations.

SECTION 2: PROHIBITED INFRASTRUCTURE USE

The Client is expressly prohibited from engaging in activities that threaten the stability, security, or integrity of the Services:

2.1 Security Circumvention: Attempting to bypass or defeat any security mechanism, authentication procedures, or rate-limiting controls.

2.2 System Abuse: Uploading or transmitting any malicious code, virus, worm, or introducing any data designed to corrupt, disable, or impair the Services.

2.3 Excessive Load: Employing automated tools to conduct disproportionate or excessive API calls or data transfers that exceed the limits of the Client's service tier and place an unreasonable, sustained load on Nokor's infrastructure.

2.4 Network Abuse: Engaging in any activity that disrupts, interferes with, or imposes an undue burden on the Services or any other client's use of the Services, including but not limited to denial-of-service attacks or orchestrated high-frequency trading that impacts system stability.

2.5 Unauthorized Access: Attempting to gain unauthorized access to the Services, related systems, or other Nokor clients' accounts or data.

2.6 Data Harvesting: Using the Services to collect or harvest Personal Data in violation of the Data Processing Agreement (DPA) or applicable privacy laws.

SECTION 3: ENFORCEMENT AND REMEDIES

3.1 Investigation: Nokor GmbH reserves the right to investigate any suspected violation of this AUP. The Client agrees to cooperate with any such investigation.

3.2 Immediate Suspension: Notwithstanding any other provision in the Agreement, Nokor GmbH may immediately suspend the Client's access to the Services upon detection of any AUP violation that poses a security risk, legal risk, or threat to the infrastructure.

3.3 Reporting: The Client shall immediately report any known or suspected violation of this AUP to Nokor GmbH at compliance@unikron.ch.

SECTION 4: GOVERNING LAW

This AUP shall be governed by Swiss law, and the exclusive place of jurisdiction shall be Schwyz, Switzerland, consistent with Article 12 of the Master ToS.