Transparency in Asset Segregation

Introduction

SmartAtlas Ltd. S.r.o. is committed to protecting client interests by ensuring the highest standards of transparency and security in the safekeeping of crypto-assets. As part of this commitment, the Company has established clear principles and procedures to segregate client holdings from its own operational and proprietary accounts. This approach is designed to provide clients with confidence that their assets are fully safeguarded, managed with integrity, and protected against risks arising from the Company's business activities.

The purpose of this document is to explain the measures implemented by the Company in relation to asset segregation, custodianship, and client reporting. It outlines the safeguards applied to prevent misuse of client assets, the internal controls and security mechanisms supporting custody arrangements, and the rights of clients to verify their balances and access transparent reporting. By doing so, the Company reinforces its regulatory obligations under MiCA and demonstrates its ongoing commitment to accountability and investor protection.

1. Segregation of Client Assets. The Company ensures that clients' crypto-assets are strictly segregated from its own holdings. All client assets are maintained in dedicated wallets separate from the Company's operational and proprietary accounts. This segregation is designed to safeguard client funds against potential financial risks associated with the Company's operations and to maintain transparency in asset management.

2. Security Measures for Crypto-Asset Protection. To ensure the highest level of security, the Company employs the following measures:

- **Cold Storage:** The majority of client assets are stored in cold wallets, which are completely offline and protected against cyber threats.
- **Multi-Signature Wallets:** Transactions require multiple authorized signatures, reducing the risk of unauthorized access or internal fraud.
- **Restricted Access Protocols:** Only a limited number of designated personnel have access to crypto-assets, and access is granted through multi-factor authentication (MFA) and strict internal controls.
- **Regular Security Audits:** The Company conducts periodic security assessments to ensure compliance with the latest security standards and industry best practices.

3. Custodianship and Limitations of Liability. The Company acts as a custodian for clients' crypto-assets, providing safekeeping services. While the Company implements rigorous security measures, it does not assume liability for external risks beyond its control, including but not limited to:

- Blockchain network failures or disruptions
- Force majeure events, such as cyber-attacks on third-party service providers
- Governmental actions or regulatory changes impacting crypto transactions

4. Client Verification and Reporting. Clients have the right to verify their crypto-asset balances at any time through the Company's secure online portal. Additionally, the Company provides:

- **Periodic Statements:** Clients receive statements confirming their holdings at regular intervals, detailing asset balances and transaction history.
- **On-Demand Verification:** Clients may request detailed reports regarding their holdings, which will be provided within the Company's designated response timeframe.
- **Audit Reports:** Upon request, clients may review audit reports demonstrating compliance with segregation and security protocols.