Custody Policy Summary

Purpose of the Custody Policy Summary

This document presents a summary of SmartAtlas Ltd. S.r.o.'s custody policy for the safekeeping and administration of client crypto-assets. It sets out the key principles, internal rules, and operational procedures designed to ensure the secure holding of assets, the transparency of custody operations, and full compliance with applicable regulatory requirements.

The summary provides clients and stakeholders with a clear understanding of how the Company safeguards crypto-assets under its management, the measures in place to mitigate risks, and the standards of accountability and governance that underpin its custody services. By doing so, the Company reaffirms its commitment to protecting client assets and maintaining trust in its role as a regulated crypto-asset service provider.

1. Safekeeping and Control of Crypto-Assets

The Company is committed to securely holding client crypto-assets, including private keys and other access credentials. Only authorized personnel have access to client assets, and access is strictly controlled through multi-factor authentication (MFA) and role-based access control (RBAC).

The Company employs a robust and multi-layered key management system to ensure the security, integrity, and accessibility of cryptographic keys:

- Multi-Signature Wallets (Multi-Sig): Cold storage wallets require approval from multiple authorized parties to execute a transaction. This threshold-based model ensures that a single compromised key cannot lead to unauthorized asset transfers.
- Hardware Security Modules (HSMs): All cryptographic keys are generated and stored within FIPS 140-2 Level 3 certified HSMs, which protect against physical and logical tampering.
- Role-Based Access Controls (RBAC): Only a predefined set of roles (e.g., compliance officer, IT security lead, operations officer) have segmented access privileges to participate in key-related operations.
- Approval Workflow:
    - Initiation: Transfer requests are initiated through internal control systems.
    - Validation: A risk engine verifies transaction parameters against AML/KYC and fraud models.
    - Authorization: Multi-signature execution is completed only after multiple signatories approve the request independently.
- Audit Logging: Every action involving private keys is logged immutably, with real-time monitoring and forensic-ready archiving.

2. Risk Mitigation Measures

The Company implements various measures to reduce risks related to fraud, cyber threats, and operational failures. These measures include continuous monitoring of transactions, encryption of sensitive data, and insurance coverage to protect against risks such as theft or loss of assets.

The company implements industry-best practices to prevent loss, theft, or unauthorized access to crypto-assets. These include:

A. IT Security Infrastructure
B. Data & Key Security
C. Operational Risk Mitigation
D. Business Continuity & Recovery

3. **Segregation of Client Assets**

Clients' assets are segregated from the Company's own assets to guarantee that the loss or insolvency of the Company does not affect client holdings. All client assets are stored in distinct and identifiable wallets to ensure clear ownership.

The Company ensures full transparency and protection of client assets through clear segregation protocols, even in cases of omnibus wallet usage:

Omnibus Wallets with Internal Ledger Segregation: While some wallets may hold funds from multiple clients for operational efficiency, the Company maintains a real-time, client-specific internal ledger that reflects each user's precise balance.

Dedicated Cold Wallets for Institutional Clients: High-volume and institutional clients may be assigned dedicated cold wallets for additional assurance and audit trail purposes.

Periodic Third-Party Reconciliation: External audits are conducted to verify that client ledger balances match actual wallet holdings, ensuring no commingling of firm and client assets.

No Proprietary Use of Client Assets: The Company does not lend, stake, or otherwise use client funds for its own operations unless explicitly agreed by the client under separate terms.

Legal and Technical Firewalls: Technical systems enforce strict separation of user and platform funds, and legal structures prohibit claims on client assets by corporate creditors.

4. **Transparency and Reporting**

Clients receive regular, clear, and accurate reports on the status, movements, and balances of their assets. These reports are provided at least every three months or upon request or can be viewed in the Client's Account. The Company provides information to clients about any events that may affect their rights or assets, including changes in asset positions or rights.

5. **Client Rights and Access**

The Company assists clients in exercising any rights attached to their crypto-assets. This includes access to and control of assets in the event of protocol changes or other relevant events. The Company guarantees that clients' rights to newly created crypto-assets (e.g., from blockchain upgrades) are preserved.

6. **Security Systems and Procedures**

The Company employs a secure, multi-tiered asset management framework to identify and manage clients' crypto-assets:

- Unique Wallet Allocation

- Wallet Management Infrastructure
- Private Key Management

7. Fees and Costs

The Company's custody services are subject to fees, which are clearly outlined in the client Agreement. These fees include charges for custody, administration, and any additional services that may be required by the client.

8. Return of Assets

In accordance with the client's instructions, the Company facilitates the prompt and secure return of crypto-assets or the means of access (e.g., private keys). The return process follows established protocols to guarantee asset security.

9. Compliance with Regulations

The Company adheres to all relevant **legal and regulatory requirements**, including **Regulation (EU) 2023/1114 (MiCA)**, ensuring that the custody and administration of crypto-assets meet all compliance standards, including segregation, reporting, and risk management.