CRYPTO CUSTODY AND ADMINISTRATION

The Crypto Custody Policy of UAB Decentralized (the Company), established in line with the European Union's Markets in Crypto-Assets Regulation (the MiCA Regulation) and the Digital Operational Resilience Act (DORA), sets out the procedures and controls for securely holding and managing Client Crypto-assets. The policy aims to reduce risks of asset loss, ensure accurate and complete recordkeeping, and provide transparency regarding the terms and risks of custody. It further outlines how the Company protects Client assets through segregation, access controls, key lifecycle management and continuity planning. The Policy is reviewed and updated regularly to reflect changes in regulatory obligations, technical infrastructure and internal practices.

KEY COMPONENTS OF THE COMPANY'S CUSTODY SERVICES

- **Security measures:** Technical and procedural controls such as multi-factor authentication, encryption of cryptographic key material, role-based access restriction and secure wallet architecture protect Client Crypto-assets.
- **User interface:** A secure and intuitive Client portal allows Clients to view balances, initiate withdrawals and manage account access with real-time updates.
- **Transaction execution:** Transactions initiated by Clients are processed through automated and manual checks to ensure compliance, accuracy and secure delivery to the blockchain.
- **Recovery services:** A recovery process involving identity verification through official documents enables Clients to regain account access if credentials are lost.
- **Customer support:** Support is provided through live chat during business hours and email, with all inquiries tracked through the Company's customer relationship management system.
- **No outsourcing of custody:** All custody decisions, private cryptographic key management, access control and transaction authorisation are performed internally by Company personnel. The Company may use a technical infrastructure provider (the Technical Provider) for the management of Cold and Deep Cold Wallets, but the Technical Provider does not hold, access or control any private cryptographic keys, and custody of Client Crypto-assets remains solely with the Company at all times.

CUSTODY SOLUTIONS

The Company provides crypto custody services as an integrated component of its operational offerings. Custody is essential for supporting cryptocurrency payments, conversions between funds and Crypto-assets, and crypto payouts made on behalf of Clients. Client Crypto-assets are held in Segregated Wallets, distinct from Company assets and fully traceable in the Company's technical and accounting systems. While Crypto-assets are pooled in Segregated Wallets, each Client's entitlements and ownership rights are accounted for individually in the Company's internal ledger.

Three types of Segregated Wallets are used:

- Deep Cold Wallets, which store the majority of Client Crypto-assets offline. Private cryptographic key material is distributed across multiple independent environments so that no single environment, device or person holds the complete private key at any time, and key material is encrypted at rest throughout its lifecycle. Access is restricted to designated senior management and transactions require quorum-based approval enforcing the four-eyes principle at the platform level. The individual who initiates a transaction cannot approve it.

- Cold Wallets, which are also offline and used for outgoing Client payments such as withdrawals and refunds. Key material is similarly distributed and encrypted. Transactions are formed programmatically by the Company's authorised systems and signed automatically by a dedicated signing component within the Company's infrastructure, with destination addresses managed through defined controls and full audit logging.
- Hot Wallets, which are internet-connected and used to receive Client deposits and process high-frequency automated transactions through the Company's internally developed crypto-asset management infrastructure (the Argus system). Private keys are managed using AWS Secrets Manager hosted in the AWS EU region, with role-based access controls, encryption and automated alerting. Balances held in Hot Wallets are minimised by periodic sweeps to other storage locations.

The Company maintains a key backup and recovery process designed to ensure continued access to Client Crypto-assets in the event of device loss, personnel unavailability or infrastructure failure. Backups are performed on a dedicated air-gapped workstation, encrypted backup packages are stored separately from the means of decryption, and the encrypted backup material and the means to decrypt it are held by different authorised personnel. No single individual can independently complete a full key recovery; the process requires the coordinated involvement of multiple authorised personnel.

All wallet types are maintained under strict operational and cybersecurity controls, including daily reconciliation, key lifecycle procedures and continuous monitoring. Custodial pooling is applied, but individual Client entitlements are recorded in real time in an internal ledger. No Company assets are held in Segregated Wallets and Client Crypto-assets are never used for Company operations.

REGISTER OF CLIENT POSITIONS

The Company maintains a secure, real-time register of Client Crypto-asset holdings in accordance with the MiCA Regulation. Each Client has a dedicated section in the register, ensuring ownership rights are distinct, traceable and accessible for reporting and reconciliation. All transactions – deposits, withdrawals and internal movements - are logged based on Client instructions and undergo thorough authentication, compliance and verification procedures before execution. Once processed, transactions are recorded with full detail and confirmations sent to the Client. Clients can access reports at any time via the Client portal and receive a monthly Statement of position outlining holdings, values and balances.

TECHNICAL ARCHITECTURE OF REGISTER AND DATA STORAGE

The Company's client position register is built on a PostgreSQL database managed via the Amazon Web Services (AWS) Relational Database Service (RDS) platform, ensuring reliability, security and high availability. The system includes two databases: the core-ledger, which records all financial transactions using the double-entry method, and the core-database, which stores related transaction and client information. The register operates on an append-only basis, preventing changes or deletions to existing records, and each transaction is time-stamped, uniquely identified and recorded in sequence. Data integrity is maintained through double-entry accounting, enforced relational links and unique indexes to prevent duplicates. Continuous backups are performed through AWS RDS in line with the Company's backup and recovery procedures.

SEGREGATION OF CLIENT ASSETS

The Company ensures all Client Crypto-assets are held in Segregated Wallets, entirely separate from the Company's own holdings. These assets remain the property of the Client and cannot be used for Company operations, investments or liabilities. Internal ledgers precisely account for each Client's entitlement, even when assets are pooled. Access to Segregated Wallets is strictly limited to designated personnel and all transactions are subject to security protocols, including multi-factor authentication and encryption. In case of accidental receipt of Client assets into operational wallets, the Company transfers them to the appropriate Segregated Wallet by the next business day. In insolvency scenarios, Client assets remain protected from claims of the Company's creditors.

RISK MANAGEMENT

The Company actively identifies, monitors and mitigates risks related to crypto custody. These include unauthorised account access, asset loss or theft, technical failures, operational errors, regulatory breaches, market volatility and third-party infrastructure risk arising from the use of the Technical Provider for Cold and Deep Cold Wallet management. Controls include encryption, multi-factor authentication, role-based access, intrusion detection and regular audits. Key management follows strict lifecycle protocols, with secure backup and quorum-based transaction approvals; private cryptographic key material is structured so that no single person or system can unilaterally access or reconstruct a full private key. Technical risks are addressed through automated monitoring, vulnerability scanning, weekly automated scanning of critical systems and tested recovery procedures. Operational resilience is supported by segregation of duties, the four-eyes principle, mandatory employee training and incident response. Third-party infrastructure risk is mitigated through contractual safeguards, periodic reviews of the Technical Provider's performance and security posture, and the Company's ability to move Client assets to in-house backup infrastructure if the Technical Provider's services are disrupted. Regulatory compliance is maintained through ongoing legal monitoring, policy updates and audit reviews aligned with both MiCA and DORA.

EXERCISE OF THE RIGHTS ATTACHED TO THE CRYPTO-ASSETS

The Company does not facilitate the exercise of rights attached to Crypto-assets held in custody, such as voting, staking, governance participation or receiving protocol rewards. In the event of a hard fork, airdrop or similar event, Clients are not entitled to any resulting rights or new assets unless the Company explicitly states otherwise. Assets are held in pooled wallets, and no individual allocation or benefit from such events is provided unless the Company elects to support them at its sole discretion.

ACCESS TO AND RETURN OF CRYPTO-ASSETS UNDER CUSTODY

Clients can securely access and withdraw their Crypto-assets at any time through the Company's encrypted Client portal, which requires multi-factor authentication. Withdrawal requests are processed through a structured and secure procedure that includes verification of wallet ownership, identity authentication and compliance checks against regulatory requirements. All access and return activities are logged, and account activity is continuously monitored to maintain transparency and support auditability. Sensitive operations, such as changing account security settings or adding new withdrawal addresses, require additional authentication. If Clients lose access credentials, they can initiate a secure recovery process involving government-issued ID verification and confirmation of account details. In certain situations, such as unsupported assets, account closure or supervisory orders, the Company may return or liquidate Crypto-assets, with advance notice provided whenever possible.

LIABILITY FOR LOSS OF CRYPTO-ASSETS

The Company is liable for any loss of Crypto-assets or means of access to them resulting from its negligence, misconduct or failure to follow agreed security protocols. Liability is limited to the market value of the lost Crypto-assets at the time of the incident, based on average prices across major Crypto-asset service providers. The Company is not responsible for losses caused by Client negligence, phishing attacks, third-party breaches of systems not connected to the Company, malfunctions inherent to distributed ledger technology, or force majeure events. If a loss occurs, the Company will investigate, document the findings and inform affected Clients. Clients must report losses within a specified timeframe. If the Company is found liable, compensation will be issued accordingly. The Company also maintains a proactive duty to implement effective security controls, provide risk disclosures, deliver employee training and maintain accurate records to prevent asset loss.