Crypto custody and administration

The Crypto Custody Policy of Decentralized, UAB (the **Company**), established in line with the European Union's Markets in Crypto-Assets Regulation (the **MiCA Regulation**), 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 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, key encryption, 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.

Custody solutions

The Company provides crypto custody services as an integrated component of its operational offerings. Custody is essential for supporting cryptocurrency payments, funds-to-crypto conversions, 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.

Three types of Segregated Wallets are used:

- Deep Cold Wallets, which store the majority of Client Crypto-assets offline on air-gapped devices. These wallets require 2-of-3 multi-signature approval and involve secure physical storage and access protocols. Key material is encrypted, backed up, and accessible only through coordinated actions of multiple authorized personnel.

- Cold Wallets, which are also offline and used for outgoing Client payments such as withdrawals and refunds. Access is limited to authorized personnel in the Company's finance team. Transactions are system-generated and require single-approval signatures.

- Hot Wallets, which are internet-connected and used to receive Client deposits and facilitate high-frequency transactions. Security is enforced through AWS Key Management Services with role-based access controls, encryption and automated alerting.

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.

Segregation of Client assets

The Company ensures all Client Crypto-assets are held in Segregated Wallets or Safeguarded Accounts, 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 or Safeguarded Accounts 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 or Safeguarded Account by the next business day or allocates equivalent assets from its own funds. In insolvency scenarios, Client assets remain protected from Company claims.

Risk management

The Company actively identifies, monitors and mitigates risks related to crypto custody. These include unauthorized access, asset theft, technical failures, operational errors, regulatory breaches and market volatility. Controls include encryption, multi-factor authentication, role-based access, intrusion detection and regular audits. Key management follows strict lifecycle protocols, with secure backup and multi-signature approvals. Technical risks are addressed via monitoring tools, vulnerability scanning, and tested recovery procedures. Operational resilience is supported by segregation of duties, employees training, and incident response. Regulatory compliance is maintained through ongoing legal monitoring, policy updates and audit reviews.

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 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 access credentials 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 exchanges. The Company is not responsible for losses caused by Client negligence, phishing attacks, third-party breaches, DLT malfunctions 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, ensure employees training and maintain accurate records to prevent asset loss.