

SEGREGATION OF CLIENT CRYPTO-ASSETS AND FUNDS

The Segregation of Client Crypto-Assets and Funds Policy of UAB Decentralized (the Company), aligned with European Union Regulation (EU) 2023/1114 on Markets in Crypto-Assets (the MiCA Regulation), sets clear standards to ensure that Client assets are protected through strict operational and legal separation from the Company's own assets. This policy outlines the internal systems, roles and procedures the Company applies to ensure the integrity, transparency and traceability of all Client-held Crypto-assets and funds. It guarantees that these assets are used only in accordance with the instructions of the Client and remain protected in the event of the Company's insolvency or operational risk events.

KEY COMPONENTS OF THE COMPANY'S SEGREGATION PRACTICES

- **Account and wallet segregation:** Client funds are safeguarded in a Safeguarded Account held with a licensed credit institution and used exclusively for the safeguarding of Client funds under Article 70 of the MiCA Regulation. A separate Settlement Account, held with an authorised Electronic Money Institution (EMI), is used solely as a technical account for receiving incoming Client deposits and executing outgoing Client withdrawals. Crypto-assets are stored in designated Segregated Wallets. Client assets are never mixed with the Company's own assets.
- **Access control:** Access to the Safeguarded Account, the Settlement Account and Segregated Wallets is restricted to authorised employees, with permissions assigned and reviewed by the CEO and CFO to ensure integrity and oversight.
- **Client reporting:** Clients receive monthly Statements summarising the status and value of their Crypto-assets and funds. Statements are available at any time through the secure Client portal.
- **Audit and monitoring:** All movements of Client funds and Crypto-assets are recorded in the Company's internal ledger with full traceability. Reconciliations are performed daily and internal audits are conducted regularly.
- **Incident management:** In the event of a segregation or safeguarding failure, the Company activates its incident response procedures, notifies affected Clients and regulators and implements remediation actions.

SEGREGATION SOLUTIONS

The Company separates Client Crypto-assets and funds from its own assets in a structured and secure way. Client funds are protected through a Safeguarded Account held with a licensed credit institution, which is used exclusively for safeguarding Client funds in accordance with Article 70 of the MiCA Regulation. The Safeguarded Account does not receive Client deposits directly and is not used to execute Client withdrawal payments; it is operationally and legally separated from the Company's own assets and protected from claims by the Company's creditors.

To process incoming and outgoing payments, the Company uses a Settlement Account held with an authorised Electronic Money Institution. The Settlement Account is a technical routing account: incoming Client deposits are received into the Settlement Account and promptly transferred into the Safeguarded Account by the end of the business day. When a Client requests a withdrawal, the required amount is moved from the Safeguarded Account to the Settlement Account solely for the purpose of executing the payment to the Client. The Settlement Account does not form part of the safeguarding structure under Article 70 and is not a Safeguarded Account.

Client Crypto-assets are held using three types of Segregated Wallets: Hot, Cold and Deep Cold. Hot Wallets handle incoming deposits and frequent transfers, Cold Wallets are used for planned outgoing payments and Deep Cold Wallets store the majority of Crypto-assets offline to increase safety. Each wallet is used only for Client assets and internal systems clearly track ownership. When deposits or exchanges occur, Client balances are updated automatically. If any delay or mistake happens, the Company ensures that Client holdings are protected by using its own resources to correct the issue.

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 are sent to the Client. Clients can access reports at any time via the Client portal and receive a monthly Statement of their Crypto-asset holdings, values and balances.

SEGREGATION OF CLIENT ASSETS

The Company keeps an accurate and up-to-date record of each Client's Crypto-assets and funds. These records are stored in the Company's internal ledger and accounting system, showing the amount and type of assets held for every Client. Each deposit, withdrawal or transaction is recorded and linked to the Client who owns the assets.

Clients receive a monthly Statement, which includes a breakdown of their assets, the account ID, asset quantities, exchange rates and other relevant details. These Statements are available through the secure Client portal and can be downloaded at any time. Clients may also request additional Statements during the year, which are provided within five business days.

INTERNAL CONTROL AND RECONCILIATION

The Company enforces internal control measures to ensure accurate recording and protection of Client Crypto-assets and funds. The CFO oversees daily reconciliations between Client balances, internal accounting records and the actual balances held in the Safeguarded Account, the Settlement Account and Segregated Wallets. Any discrepancies are identified and resolved promptly, with actions documented for transparency. The Company's systems generate daily reports detailing Client balances, transactions and the state of the Safeguarded Account, the Settlement Account and Segregated Wallets. These reports confirm that Client assets are always correctly allocated and remain separated from the Company's own resources.

Access to Client accounts is strictly limited to authorised personnel. Separation of duties ensures that no single employee can manage the full process, supporting accountability and reducing the risk of error or misuse. The Compliance Officer and Internal Auditor review the segregation and safeguarding processes periodically, providing independent oversight and recommending improvements.

If Client funds or Crypto-assets are mistakenly received into non-designated accounts, they are transferred to the appropriate segregated location without delay. Conversely, if the Company's own funds or non-Client funds are mistakenly received into the Safeguarded Account or the Settlement Account, they are identified and removed promptly. In cases where this cannot be done immediately, the Company uses its own funds or assets to ensure the Client's position remains protected.

WITHDRAWAL AND RETURN OF ASSETS

Clients can request the withdrawal of their funds or Crypto-assets through the Company's platform. Each request is subject to identity verification before being processed. Withdrawals are executed based on the type of asset: for Client funds, the required amount is first transferred from the Safeguarded Account to the Settlement Account solely for the purpose of executing the Client's payment instruction, and from there disbursed to the Client's designated bank account. For Crypto-assets, the required amount is sent from the relevant Segregated Wallet to the Client's designated wallet address.

Each withdrawal is fully logged and all transactions are tracked from initiation to completion. The process ensures asset traceability and transparency, confirming that Client assets remain properly separated and are never used to fulfil other obligations.

LIABILITY FOR ASSET MISMANAGEMENT

The Company is responsible for maintaining the safety of Client Crypto-assets and funds held in its custody. If any loss or mismanagement occurs due to internal errors, system failures or failure to follow established procedures, the Company may be held liable, subject to investigation outcomes. The Company is not responsible for losses resulting from Client actions, such as providing incorrect wallet details, failing to secure personal credentials or unauthorised third-party access outside the Company's systems. In the event of an incident, the Company investigates and communicates findings to affected Clients and to the relevant authorities where required.

STATEMENT

The Company provides Clients with a monthly Statement summarising their held assets, including but not limited to asset types, account IDs and ending balances. Statements are issued within ten business days of each month's end and are securely accessible via the Company's encrypted Client portal. Clients may request additional Statements at any time and the Company will deliver them within five business days. These reports help ensure transparency and allow Clients to verify their positions and transaction history at any time.