UAB Star Ventures

Policy on Segregation, Custody and Administration of Crypto-assets

1. Version control

VERSION	DATE	Description
1.0		Creation of Policy

Table of Contents

2. General provisions

2.1. The purpose of the Policy on Segregation, Custody and Administration of Crypto-assets (the "**Policy"**) is to provide measures and procedures applied by the Company in order to ensure that Customer's Crypt-assets are always kept separate from the Company's operational and proprietary assets, minimizing the risk of loss or misappropriation. Policy also outlines the measures the Company employs to protect Customer's Crypto-assets in the event of financial difficulties, such as insolvency or bankruptcy. Further, the Policy ensures that the services of custody and administration of the Crypto-assets on

behalf of Customers are provided securely, in compliance with the applicable legal acts and regulatory requirements, including, but not limited to, the Regulation (EU) 2023/1114 of European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (the "**Regulation**"), as well as the technical standards submitted by the European Securities and Markets Authority, specifying the requirements of the custody and administration services set out in the Regulation (both the Regulation and the technical standards - the "**Legislation**").

3. Used terms

3.1. **Company** – UAB Star Ventures.

3.2. **Crypto-assets** – means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology which are supported by the Company. A full list of the Crypto-assets the Company supports can be found on the website of the Company (https://www.coinpayments.net/supported-coins-all) .

3.3. **Customer** – a legal person to whom the Company provides services.

3.4. **CEO (Chief Executive Officer)** – the person elected by the Management Board of the Company, who organizes everyday Business activities of the Company within the limits of his / her powers.

3.5. **ICT** - **Information** and Communication Technology (ICT).

3.6. **Management Board** – collegial management body of the Company.

3.7. Other terms used in this Policy are understood as defined in the legal acts and Governance Arrangements Policy of the Company.

4. General principles

4.1. The Customers' Crypto-assets shall be kept segregated from the Company's operational and proprietary assets. This segregation guarantees that Customers' Crypto-assets are not commingled with the Company's own assets and are safeguarded from risks associated with the Company's business operations. The Company strictly adheres to the requirement not to use Customers' Crypto-assets in its daily operations at any time during its activities.

4.2. Customers' Crypto-assets are stored in segregated omnibus wallets, with detailed internal records tracking ownership and ensuring accurate account reconciliation.

4.3. The Company performs periodic reconciliations of all Customers' Crypto-assets, comparing internal records with external blockchain data to maintain precise accounting.

4.4. All Crypto-assets held in custody remain the legal property of the Customers at all times.

4.5. In the event of insolvency or bankruptcy, Customers' crypto-assets will be legally and operationally segregated, ensuring they remain protected from creditor claims and accessible to Customers.

4.6. The Company ensures that Customers can fully exercise their rights over their Crypto-assets, including withdrawals, transfers and monitoring of balances.

4.7. All details on Customer's Crypto-assets and detailed account history are available to the Customer at all times in the Customer's profile on the Company's platform as well as in downloadable PDF format.

4.8. The Company, as the custodian and administrator of Customers' Crypto-assets, is liable for any loss of assets or means of access due to an incident attributable to the Company, with liability capped at the market value of the lost asset at the time of loss.

5. Types of Custody and Segregation from the Company's Assets

5.1. The Company provides custody services to ensure the secure and reliable safekeeping of Customers' Crypto-assets. These services include the segregated custody of both Customers' and the Company's crypto-assets, utilizing CoinPayments Inc.'s software infrastructure.

5.2. The Company ensures that the Crypto-assets of the Customers held in custody are operationally segregated from the Company's estate. Customers' and Company's proprietary Crypto-assets are securely stored in omnibus wallets per blockchain network, strictly ensuring that Customers' and the Company's Crypto-assets remain distinct at all times across all transactions and balances. The Company maintains separate omnibus wallets for:

5.2.1. Customers' crypto-assets, held in segregated wallets exclusively for Customer holdings;

5.2.2. Company's operational crypto-assets, maintained in separate wallets for internal operations and liquidity management.

5.3. The Company employs a dual-layer custody approach, utilizing both cold wallets and hot wallets for different operational needs:

5.3.1. Cold wallets: designed for long-term safekeeping, minimizing exposure to external threats by keeping assets in offline storage;

5.3.2. Hot wallets: used for real-time deposits and withdrawals, facilitating efficient transaction processing while maintaining security controls.

5.4. The custody framework operates in a way that individual private keys are not assigned to each Customer. Instead, the Company maintains full control over the omnibus wallets, with a secure internal ledger system that accurately tracks each Customer's balance and transaction history, as detailed further in Sections 6 and 7 below.

5.5. Customers retain full legal ownership of their Crypto-assets at all times. These assets shall not, under any circumstances, be considered part of the Company's proprietary holdings. The Crypto-assets of the Customers are accounted off-balance sheet of the Company, ensuring the avoidance of commingling of Customers' Crypto-assets with the

Company's assets as well as protection from mismanagement, claims, or insolvency impact on such Crypto-assets of the Customers. The Company follows strict internal controls and maintains detailed records of ownership to ensure continuous compliance with legal and regulatory frameworks.

5.6. The Company may hold a part of its own Crypto-assets with the liquidity providers to facilitate operational activities such as Crypto-asset conversion through the third-party execution venues. These holdings belong to the Company and are not subject to the segregation and custody rules applicable to Customers' Crypto-assets.

6. Segregation of Crypto-Assets Between the Customers

6.1. The Company maintains segregated omnibus wallets based on blockchain networks and asset types. These omnibus wallets contain pooled holdings from multiple Customers, yet they are structured to ensure clear and accurate ownership records for each individual Customer.

6.2. The Company's system tracks every transaction - including incoming deposits, outgoing withdrawals, and internal transfers - and records them against the respective Customer's account balance. This system ensures that:

6.2.1. a dedicated ledger is maintained for each Customer, recording all balances and transactions;

6.2.2. every transaction is precisely attributed to a specific Customer, preventing misallocation;

6.2.3. an aggregated ledger reflects the total balance of all Customer holdings, which matches the total assets held in omnibus wallets.

6.3. The internal ledger system ensures that Crypto-assets belonging to the Customers are segregated both from the Crypto-assets of other Customers as well as from the Crypto-assets of the Company and are not used for the Company's own account.

7. Reconciliation of Customers' Crypto-Assets

7.1. Regular reconciliations are performed to ensure that the Company's internal records accurately reflect actual asset holdings. This practice guarantees that any discrepancies are promptly identified and corrected, maintaining the integrity of Customers' crypto-assets. To uphold financial security, the Company ensures that the total amount of crypto-assets held in custody is always equal to or greater than the aggregated balance of all Customers' assets, preventing any possibility of cross-utilization between accounts.

7.2. To achieve precise accounting, periodic reconciliations are conducted by the Financial Controller (if the Financial Controller is not appointed or cease to be appointed within the Company, then the responsibilities of it shall be undertaken by the CEO). This process involves capturing a snapshot of all Customer balances at a designated moment while simultaneously recording the balances held within all wallets, maintaining Crypto-assets of the Customers. The aggregated balances of these records are then compared and the results are documented to verify accuracy.

7.3. Apart from periodic reconciliation indicated in Clause 7.2 above, Crypto-asset reconciliation checks are conducted automatically during operations that involve the movement of the Crypto-assets, ensuring accuracy and security in asset management. These checks are triggered whenever the Crypto-assets are sent out on the blockchain,

whether as a result of Customer transactions or internal transfers to cold wallet storage for safekeeping.

7.4. In the event of unexpected discrepancies, the Company undertakes immediate investigation to determine the cause. If the investigation confirms a shortage attributable to the Company, the necessary corrective measures shall be undertaken without delay, including transferring the required amount of Crypto-assets to rectify the discrepancy.

8. Rights of the Customers. Multi-signature Approval System

8.1. The Company is committed to enabling Customers to fully exercise their rights attached to the Crypto-assets held in the custody of the Company. These rights include the ability to exchange Crypto-assets for other Crypto-assets, deposit Crypto-assets into the custody of the Company or transfer / withdraw the Crypto-assets to the external platforms at any time. The User Agreement as well as other internal policies of the Company elaborate further on the rights of the Customers and the procedures for exercising their rights as well as utilizing the services of the Company related to the Crypto-assets, including conversions, deposits and transfers/withdrawals.

8.2. Under the custody model managed by the Company, the Crypto-assets are maintained in omnibus wallets that are segregated per blockchain network, ensuring a clear distinction between Customers' assets and the Company's proprietary holdings. These omnibus wallets are further categorized into hot wallets, which facilitate real-time transactions, and cold wallets, designed for long-term safekeeping:

8.2.1. to facilitate seamless and efficient transaction processing, Customer deposits and withdrawals are fully automated. Withdrawals initiated by Customers are executed instantly through the hot wallet system without manual intervention. However, for enhanced security and risk management, the Company has established predefined withdrawal thresholds, beyond which transactions require additional verification. In the case of large withdrawals that exceed the predefined limit, manual confirmation by designated personnel is triggered before execution, ensuring enhanced scrutiny of high-value transactions;

8.2.2. cold wallets serve as the primary storage for long-term holdings, minimizing exposure to security risks. A multi-signature approval system is implemented for the release of assets from cold storage, requiring multiple authorized signatories to approve transactions before the Crypto-assets can be moved to the hot wallet for withdrawal processing. This ensures that no single individual has unilateral control over the release of Crypto-assets from cold storage, thereby strengthening the security and integrity of the custody framework.

9. Customers' Position Register

9.1. Based on the internal ledger records set out in Clauses 6.1-6.3, the Company maintains a comprehensive position register that records each Customer's rights to the Crypto-assets held in custody. This register is meticulously managed to ensure that all holdings are accurately attributed to individual Customers, allowing for complete traceability and transparency. Every transaction, whether a deposit, withdrawal, or internal transfer, is promptly recorded, ensuring that all movements of crypto-assets are fully documented and regularly updated. The register serves as a clear and auditable record, safeguarding the integrity of each Customer's balance and transaction history.

9.2. To uphold accuracy and reliability, the Company performs regular reconciliations, comparing the recorded Customer positions in the position register with actual holdings in custody as defined in section 7.

9.3. The Company does not own, control, operate, or maintain the underlying distributed ledger technology governing the Crypto-assets it supports. Blockchain protocols are open-source and subject to changes, including network forks, upgrades and other modifications that may create or alter a Customer's rights. Where changes to the underlying distributed ledger technology or any other event are likely to create or modify a Customer's rights, the Customer shall not be entitled to any newly created Crypto-assets or rights arising from such events. This applies to the extent of the Customer's positions at the time of the occurrence of such changes, following the Customer's waiver of entitlement to forked crypto-assets as set forth in the User Agreement.

9.4. In instances where the Company becomes aware of an upcoming change to the underlying distributed ledger technology that may create or modify a Customer's rights - such as a planned blockchain fork - the Company will, where possible, notify Customers in advance and provide an opportunity to withdraw their Crypto-assets before the fork occurs. The Company does not guarantee such warnings in all cases, particularly where changes occur suddenly, without prior announcement, or in a manner that does not allow for reasonable notice.

9.5. The Company will update the Customer's position register to reflect the occurrence of a fork without assigning any new assets to the Customer. The position register may contain a record indicating that a blockchain fork occurred at a specific block height, along with a statement that the newly created chain or asset is not supported by the Company and is therefore not reflected in Customer balances. This ensures transparency while maintaining consistency with the terms of the User Agreement.

9.6. At its sole discretion, the Company may decide to support modifications to Customer rights resulting from changes in the underlying distributed ledger technology. If the Company opts to recognize a newly created Crypto-asset or right, Customers who would have been entitled to such assets or rights based on their holdings at the time of the event will be notified accordingly. The Company will update the Customer's position register to reflect the assigned assets or rights, ensuring proper reconciliation and transparency.

9.7. All details on Customer's Crypto-assets held in the Customer's name, their balance, their value and detailed account history, including the transfer of Crypto-assets made during the period concerned, are available to the Customer at all times in the Customer's profile on the Company's platform as well as in downloadable PDF format.

10. Systems and Controls to Manage Operational and ICT risks

10.1. The Company recognizes that the provision of custody and administration of Crypto-assets involves operational risks and Information and Communication Technology(ICT) risks that could impact the safekeeping and control of Customers' crypto-assets. The following risks have been identified:

10.1.1. Coercion or unauthorized actions by internal personnel - the risk that authorized personnel with access to multi-signature keys may be coerced or act maliciously to misappropriate funds;

10.1.2. Malicious insider threats - individuals with administrative access could attempt to misdirect funds that have not yet been transferred to cold storage;

10.1.3. IT infrastructure vulnerabilities - security breaches, cyberattacks or infrastructure failures may compromise private keys, transaction integrity and Customer balances;

10.1.4. Loss of cryptographic key components - if cryptographic keys are compromised, lost, or stolen, unauthorized withdrawals or permanent loss of access to assets may occur;

10.1.5. Denial-of-Service (DoS) and anomaly attacks - external parties may attempt to disrupt services through DoS attacks or exploit vulnerabilities in transaction monitoring systems;

10.1.6. Operational failures and business continuity risks - system downtime, data corruption, or failures in reconciliation processes could lead to inaccurate Customer balances and delayed transactions;

10.1.7. Unintentional transaction processing errors, attributable to the Company;

10.1.8. Blockchain Integration and Monitoring Failures - inadequate management of blockchain protocols, consensus rules, forks, and smart contract interactions, combined with insufficient transaction monitoring, can lead to undetected theft, double-spend attacks, loss of forked assets, trapped funds in cross-chain transfers, or exploitation of protocol vulnerabilities, resulting in permanent loss or unauthorized movement of customer digital assets;

10.1.9. Comingling of Company's own Crypto-assets with the Crypto-assets of the Customers';

10.1.10. Use of the third-party software infrastructure.

10.2. To mitigate the identified operational and ICT risks, the Company has implemented a multi-layered security and risk management framework, which includes:

10.2.1. Multi-Signature (Multisig) Key Management for Cold Storage Withdrawals:

10.2.1.1. Access to cold storage wallets is secured through a multi-signature approval system, ensuring that no single individual can unilaterally authorize transactions;

10.2.1.2. Only designated personnel approved by Company management are assigned private keys, with required authorization thresholds defined for each transaction;

10.2.1.3. Transactions involving cold storage fund releases must be approved by a predefined number of signatories before being executed.

10.2.2. Network Security and Encryption Measures:

10.2.2.1. Encryption-at-Rest and In-Transit: cryptographic keys and transaction data are encrypted using industry-standard protocols to prevent unauthorized access;

10.2.2.2. Denial-of-Service (DoS) Mitigation: the Company employs Path-based security solutions to monitor and prevent automated attack attempts on the platform;

10.2.2.3. Automated Account Lockout: Customers attempting multiple failed authentication attempts are automatically locked out to prevent brute-force access attempts.

10.2.3. Continuous Monitoring and Incident Response:

10.2.3.1. Real-Time Anomaly Detection: automated monitoring systems are in place to track unusual transaction behavior, with alerts sent to security teams for immediate investigation;

10.2.3.2. Administrative Freezing of Balances: if fraudulent or suspicious activity is detected, administrators have the ability to freeze specific Customer balances to prevent unauthorized transactions.

10.2.3.3. Incident Response & Forensic Analysis: any security breach is promptly investigated, with corrective measures implemented to prevent recurrence.

10.2.4. Operational Security and Internal Control Measures:

10.2.4.1. Role-Based Access Controls (RBAC): system administrators and operational personnel have restricted access based on their roles, reducing the risk of unauthorized transactions;

10.2.4.2. Background Checks for Key Personnel: individuals with access to cryptographic keys undergo security vetting before being granted access;

10.2.4.3. Large Withdrawal Approval Process: any withdrawal exceeding predefined thresholds requires manual approval by an administrator to ensure compliance.

10.2.5. Business Continuity and Disaster Recovery:

10.2.5.1. Automated Data Backups and contingency plans to restore operations in the event of data corruption, cyberattacks, or system failures as further defined in the Business Continuity Plan of the Company.

10.2.6. Segregation of the Crypto-assets:

10.2.6.1. Storage of Customers' Crypto-assets in segregated omnibus wallets, with detailed internal records tracking ownership and ensuring accurate account reconciliation, following with principles set out in this Policy.

10.2.7. Third-party and Outsourcing of software infrastructure:

10.2.7.1. comprehensive evaluation – assessing potential business partners based on economic, legal, and regulatory criteria, including their reputation, operational capabilities, financial stability and compliance status;

10.2.7.2. due diligence and monitoring – conducting continuous due diligence on third-party service providers to proactively identify and manage risks associated with their operations;

10.2.7.3. control of third-party providers – implementing oversight mechanisms to ensure third parties comply with contractual obligations, regulatory requirements, and the Company's internal standards;

10.2.7.4. diversification of outsourcing providers – ensuring that the Company does not rely exclusively on a single entity for critical services by assessing the feasibility of outsourcing to multiple providers; alternatively, ensuring the business continuity in case of moving to the alternative software infrastructure provider;

10.2.7.5. contractual safeguards – establishing robust contractual arrangements to clearly define service expectations, obligations and resilience standards for third-party providers;

10.2.7.6. digital operational resilience framework – implementing a structured approach to managing third-party risks in line with the DORA, ensuring external providers adhere to the same resilience standards as the Company.

10.3. Further measures implemented by the Company are addressed in the ICT Risk Management Policy of the Company and its annexes, the Risk Management Policy and the Business Continuity Plan of the Company.

11. Liability for the Loss of Customers' Crypto-assets

11.1. The Company recognizes its liability to the Customers for the loss of any Crypto-assets in custody due to an incident attributable to the Company. This ensures that Customers are protected in cases where the Company's actions or operations directly cause the loss. However, the scope of this liability is limited to the market value of the lost Crypto-assets at the time the loss occurred, providing clear parameters for compensation.

11.2. The Company is not responsible for incidents that arise independently of its operations or outside its control. For example, the Company cannot be held liable for technological issues inherent to the operation of any blockchain/distributed ledger technology that the Company does not manage or influence. Similarly, external events unrelated to the Company's systems, processes, or personnel fall outside the scope of its liability.

11.3. In the event of a loss attributable to the Company, the Company is committed to covering the loss using its own resources.

12. Disclosure of Information

12.1. The Company is committed to providing Customers with any relevant information about operations involving their Crypto-assets that may require a response or action from them. This information will be provided as soon as possible, ensuring that Customers are promptly notified of any events that might necessitate their attention or decision. The Company ensures that communication is clear, transparent, and timely, in line with the Customer's right to be informed about their holdings and any changes that may affect them.

12.2. The Company also ensures that any Crypto-assets are promptly returned to the Customer upon request. This includes the immediate processing of any transfers or withdrawals requested by the Customer.

12.3. If the Company decides to provide custody and administration of Crypto-assets on behalf of Customers by using other crypto-asset service providers for such service(s), it shall inform the Customers about this. The Company shall ensure that such a third-party service provider is authorized to provide custody services of the Crypto-assets on behalf of the Customers under the Regulation.

13. Final Provisions

13.1. The CEO shall be responsible for the implementation of the Policy. The CEO shall be entitled to appoint an employee for implementation of the Policy or certain part thereof.

13.2. At least once per year or when the circumstances (e.g. changes in applicable law etc., deficiencies in the Company activities established etc.) requires:

13.2.1. the implementation of the Policy shall be reviewed and respective report issued; and

13.2.2. the Policy shall be reviewed to make sure that it corresponds to the law applicable to the Company's activities and Company's business strategy, and, if necessary, respective changes shall be initiated.

13.3. This Policy enters into effect once approved by a decision of the Management Board, unless the Management Board decision prescribes a different date of the Policy coming into effect.