Information on Security Systems and Custody Strategy

A. Custody Strategy

Tangany GmbH ("**Tangany**") provides crypto custody services (custody, administration and safeguarding of Crypto Assets and cryptographic instruments including associated Private Keys), as well as transfer services ("**Custody Services**") to customers.

Tangany renders Custody Services on the basis of cooperation agreements ("**Cooperation Agreements**") entered into with crypto asset service providers, operators of crypto trading platforms, and cryptocurrency brokers ("**Platform**"). Under the Cooperation Agreement, Tangany is compensated for providing Custody Services to the Platform's customers.

Tangany's custody strategy is strictly limited to the safekeeping of Crypto Assets and cryptographic instruments for customers of Platforms, enabling those Platforms to execute orders and other transactions involving Crypto Assets on behalf of their customers.

Tangany does not provide Custody Services for Crypto Assets or cryptographic instruments independently of Platforms, nor does it plan to do so.

B. Security Systems Used

Tangany GmbH ("**Tangany**") has implemented the following safeguards, systems, and procedures ("**Security Systems**"):

1. Security Measures and Protective Controls

To ensure the secure custody of Crypto Assets and cryptographic instruments, Tangany employs a range of technical systems and protective measures, including the following:

a) Custody Technologies

Multiparty Computation (MPC): A technology used to generate, store, and use cryptographic signature keys to protect Crypto Assets and cryptographic instruments. Keys generated and used in MPC are never stored in a single location. Instead, each key is created in such a way that its components are split between two or more parties, with no party able to view more than its own meaningless fragment. The signing process is conducted without ever combining the key fragments. This prevents attackers from extracting sensitive material by compromising a subset of systems. In addition, each MPC participant must verify the transaction in accordance with policy, making it impossible to bypass safeguards designed to prevent key misuse.

Hardware Security Modules (HSM): Cryptographic keys are stored in a secure, tamper-resistant environment. The signing key cannot be extracted and can only be used for signing purposes. HSMs are a fundamental part of modern banking infrastructure.

b) Wallet Types

Cold Wallets: Crypto wallets that are not continuously connected to the internet. These systems are particularly protected and isolated. Their predominantly offline nature makes them less susceptible to online attacks, offering a high level of security for the storage of Crypto Assets and cryptographic instruments.

Warm Wallets: Crypto wallets used for interacting with other parties, such as brokers (for the buying and selling of cryptocurrencies). These wallets are typically characterized by a higher

degree of automation.

2. Separation between Customers' Crypto Assets and Cryptographic Instruments and Tangany's Own Crypto Assets

The Crypto Assets and cryptographic instruments held in custody by Tangany on behalf of its Customers are strictly segregated operationally from Tangany's own Crypto Assets and cryptographic instruments. The Crypto Assets and cryptographic instruments held in custody for Customers are always attributable to those Customers, who retain ownership of them at all times.

To ensure this separation, Customer Crypto Assets and cryptographic instruments are held in collective custody. For each Platform, a separate Omnibus Wallet is established in which the Crypto Assets and cryptographic instruments of that Platform's customers are jointly held. The allocation of individual Customer ownership rights in the Omnibus Wallet is maintained through an internal accounting system.

In the event of Tangany's insolvency, the Crypto Assets and cryptographic instruments can be clearly attributed to the Customer and are subject to segregation by the insolvency administrator.

Tangany does not use Customer Crypto Assets or cryptographic instruments for any other purposes — such as lending or staking — without the Customer's explicit consent.

Tangany employees are not permitted to obtain ownership of, or possession of, any Customer Crypto Assets or cryptographic instruments held in custody by Tangany.

3. Contingency and Recovery Plans

Tangany maintains contingency and recovery plans for the custody solutions described in section 1. This includes an emergency recovery plan for the Internal Booking System, which ensures that customer holdings can be accurately attributed to each Customer. These plans are reviewed regularly for accuracy and updated as necessary.

4. Transparency Requirements

Tangany, as a crypto custodian, is obligated to provide its Customers with information on their current holdings in custody at least once every three months, and upon request. These statements are provided to Customers free of charge. They show the custodial assets held, the account balance, and the value of the assets over the relevant period.

Tangany is not obliged to participate in events on the underlying DLT that would grant new rights to Customers. Such events may include a "Fork", where a blockchain splits into one or more branches and new Crypto Assets are created, or "Airdrops", where new Crypto Assets are distributed to the Platform's omnibus wallet. In such cases, allocation to individual Customer Accounts is not possible.

Risks associated with crypto custody are described separately in the section "Information on Risks Related to Crypto Custody and Transfer Services."

Information on prices and fees can be found in the "Fee and Service Schedule."

5. Risk Management and Control Procedures

Tangany has implemented comprehensive strategies and procedures to ensure the secure handling of Crypto Assets and cryptographic instruments, and to actively minimize associated risks. The specific control mechanisms include the following measures:

a) Information Security System

A structured information security system ensures compliance with protection objectives including availability, integrity, confidentiality, and authenticity. Regular risk assessments and threat evaluations are integral to maintaining the continuity and reliability of the technical and organizational security safeguards.

b) Secure Software Development Lifecycle

Our products are developed within a Secure Software Development Lifecycle (SSDLC). By integrating security controls at every development stage, Tangany aims to identify and mitigate security risks at the earliest possible point.

c) Technical Infrastructure Safeguards

Tangany's technical infrastructure is protected through a range of safeguards. These include firewalls, encryption technologies, access controls, and continuous monitoring, all of which enable early detection of and response to security-relevant incidents.

d) Internal Safeguards and Four-Eyes Principle

Security-critical processes are supported by internal safeguards and the four-eyes principle. This approach ensures that all security-sensitive actions are reviewed by at least two authorized individuals, reducing the risk of error and abuse.

e) Regular Staff Training

Tangany employees receive regular training and awareness sessions on current security topics. These sessions cover best practices in handling Crypto Assets and cryptographic instruments, and adjustments in response to evolving threats and new security requirements.

f) Regular Audit of Internal Control System

The Internal Control System (ICS) is continuously reviewed to ensure the effectiveness and compliance of all security policies and procedures. Both internal and external audits are conducted to assess existing safeguards and make necessary improvements.

6. Transaction Monitoring

Tangany performs risk-based monitoring of crypto asset and cryptographic instrument transfers, both during and after execution, based on defined criteria. These criteria are reviewed regularly and adjusted if needed. To fulfill these requirements, Tangany utilizes data analysis systems that assess Customer transfer data using predefined rules and rely on both current and historical transactions.