Cryptosmart S.p.A.

Summary description of the content of the Policy relating to the custody and administration of crypto-assets on behalf of Clients

1. General Provisions

This document summarises the content of *the policy* (the "Policy") adopted by Cryptosmart S.p.A. ("Cryptosmart" or the "Company") regarding the custody and administration of crypto-assets on behalf of clients, pursuant to Regulation (EU) 2023/1114 ("MiCAR"), with particular reference to Article 75 and the applicable provisions. The Policy is the framework through which the Company ensures the proper, secure and transparent provision of the service to its users.

2. Purpose and general principles

The purpose of this Policy is to define a technical and organisational framework aimed at guaranteeing the security, segregation and full ownership of the crypto-assets entrusted by clients, whilst ensuring compliance with European regulatory requirements. It governs the relationship between the Company, in its capacity as a custodian, and each client, setting out the procedures for managing *wallets*, private keys, related funds and the execution of instructions provided by the client.

3. Nature of the service and *assets* held in custody

Cryptosmart provides a custody service consisting of holding, on behalf of clients, crypto-assets and the related means of access (in particular private cryptographic keys), whilst also enabling the administration of such assets in accordance with instructions given by users. The crypto-assets in question include both those with an identifiable issuer and decentralised ones (e.g. Bitcoin).

The Company does not hold the crypto-assets directly, but rather stores and protects the keys required to access and use them. Management is carried out through a combination of *hot wallets* and *cold wallets*, all in *omnibus* form. The former, connected to the internet, are intended for day-to-day operations; the latter, *which are offline*, are used for long-term custody.

4. Security and *wallet* management

The Company adheres to high *standards* of cyber security. *Cold wallets* utilise a *multi-signature* structure (3 out of 6 signatures) and include physical *backups* stored in safety deposit boxes at authorised banking institutions. Signatures may be applied either via dedicated *offline* workstations or via dedicated mobile devices kept *offline* through the exchange of QR codes, ensuring there are no network connections between the *offline* and *online* environments. In the event that one of the signatories leaves the Company, the Company will replace the keys and transfer the *assets* within five working days.

Hot wallets, on the other hand, are managed using HD wallet technology in accordance with the BIP32/BIP44 standards, and for certain crypto-assets via the Fireblocks platform, with cryptographic protection and distributed control. The system allows the generation of unique addresses for each client and also provides for the *backup* of keys via Bitwarden, with multi-factor authentication and emergency access.

An automatic mechanism is in place which, once certain thresholds are exceeded, transfers excess crypto-assets from *hot wallets* to *cold wallets* ("MoveFundsFromHotToColdWallet"), thereby limiting the risks associated with keeping *assets* online.

5. Traceability, reconciliation and segregation

All crypto-assets and client funds are recorded in dedicated *databases* and are subject to daily reconciliations, verifying that individual positions match actual holdings.

Segregation is guaranteed both operationally and legally: clients' *assets* are never commingled with those of the Company, do not form part of the Company's insolvency estate and are exempt from enforcement actions by third parties. The Policy also prohibits the unauthorised use of clients' crypto-assets.

6. Management of deposits and fiat funds

Clients may deposit crypto-assets via dedicated addresses. The BlockSync IT system constantly monitors the *blockchain* and, following a minimum number of confirmations, records the deposit and updates the client's profile.

Funds (e.g. euros derived from the sale of crypto-assets) are deposited into segregated current accounts held in the clients' names at Intesa San Paolo S.p.A., Credito Emiliano S.p.A. and Poste Italiane S.p.A. The management process includes a signature mechanism involving four senior internal officers (two payment authorisers and two account signatories) and rigorous daily reconciliation checks.

7. Staking

The Policy also governs the custody of crypto-assets used in *staking* services, with different procedures for Ethereum (use of *'withdrawal* credentials'), Cardano and Polkadot (separate *wallets*, *multisig* approval and selection of validators based on objective criteria such as low fees, *self-stake* and *reward points*). For Polkadot, the selection of validator nodes requires specific *offline* ratification by the signatures of at least three authorised individuals.

8. Cybersecurity and regulatory compliance

The Company adopts a security framework that complies with the DORA Regulation, comprising:

- encryption of data in transit and at rest;
- anti-fraud monitoring and advanced *logging*;
- business continuity and *disaster recovery* plans;
- regular *audits* and vulnerability *testing*;
- three-factor authentication for withdrawal transactions (login, email code and OTP via Google Authenticator).
- ongoing staff training.

The *cloud* infrastructure used (e.g. Vultr, Digital Ocean) is redundant and complies with *the* highest security *standards*.

9. Access to information, transparency and reporting

The Company guarantees clients continuous access to balances and transaction history via the secure client portal, with the option to export statements. Notification systems are also in place, along with prompt communications in the event of extraordinary circumstances and the provision of pre-contractual information in a clear and comprehensible format.

10. Liability and client protection

The Company is liable to customers in the event of a loss attributable to its own omissions or negligence, with compensation limited to the market value at the time of the event. Liability is excluded for events of force majeure (e.g. attacks on *the blockchain*, wars, natural disasters) or events beyond the Company's control. In the event of extraordinary circumstances, the Company undertakes to provide prompt documentation proving its non-involvement in the events.

11. Right of Disposal

The Client has the right to dispose of their crypto-assets and funds held in custody at any time, subject to security and anti-money laundering controls. Instructions are executed by the end of the next working day, subject to the technical processing times of the intermediaries.

12. Periodic review and accessibility

The Policy is approved by the Board of Directors and is subject to annual review or review in the event of significant regulatory changes or substantial amendments to the Service model. A summary is published on the Company’s website and is available on request in an accessible format. The Policy is also made available to the relevant supervisory authorities for review in accordance with Articles 62 et seq. of MiCAR.