Description of Omnibus Wallets, the associated risks and the safeguards adopted by the Company

1. Description of Omnibus Wallets

The custody service is provided using a model based on the use of Omnibus Wallets, i.e. digital wallets in which crypto-assets belonging to multiple Users are held, with individual positions recorded by name in the Position Register.

This register, maintained by the Company and updated in real time, makes it possible to identify each User's balance and rights in respect of the custodied crypto-assets, even in the absence of *on-chain* segregation for individual Users via individual *blockchain* addresses.

Users' crypto-assets are therefore held within shared *wallets*, but the relevant positions are segregated and attributed by name within the Company's internal systems. In this sense, the model distinguishes between the technical aspect of custody, in which crypto-assets are aggregated within one or more omnibus wallets, and the accounting and legal aspect of ownership, in which the holdings attributable to each User are recorded separately in the Positions Register.

From an operational and security perspective, the custody infrastructure combines the use of *cold wallets* – which are not connected to the internet and are primarily intended for the storage of crypto-assets – with *hot wallets*, which are connected to the Company's operational infrastructure and are used to manage day-to-day operations. All *wallets* used by the Company are of the *omnibus* type; individual holdings are tracked via the Positions Register, which is updated in real time, and the generation and management of private keys are subject to enhanced security controls.

This model does not involve the transfer of ownership of the crypto-assets to the Company. Cryptosmart acts solely on instructions given by the User; it does not become the owner of the custodied crypto-assets and does not use them for its own account. Users' crypto-assets and funds are segregated from the Company's assets, both operationally – through the use of *wallets* and accounts dedicated to users that are distinct from those of the Company – and legally and accountingly, through registered records and separate accounts certifying users' rights.

2. Risk profiles and controls adopted by the Company

Concentration risk

Any operational or security incident affecting an *omnibus wallet* could have an impact on a large number of Users.

Controls in place – the Company holds the majority of its crypto-assets in *cold wallets* featuring multi-signature (*multisig*) systems. Furthermore, the Company applies maximum holding limits on hot wallets, automatically transferring any excess funds not required for day-to-day operations to cold wallets. This limits the amount of crypto-assets exposed *online* and reduces the potential impact of any events affecting the operational *wallets*.

Risk associated with internal recording systems

In the Omnibus Wallet model, the correct allocation of assets to individual Users depends on the proper functioning of the internal systems used by the Company to record transactions and update the Position Register. A malfunction in these systems could lead to errors in the allocation of positions.

Controls in place – the Company maintains a Positions Register for each User; carries out periodic reconciliations, at least daily, between the results of its systems and the balances actually held; maintains the traceability of transactions via *an audit trail*; maintains *backups* of the Positions Register; applies operational and second-level controls; and adopts procedures for managing anomalies, adjustments and verifications. Consequently, both the Company and the User can verify the relevant balances at any time.

Risk of individual on-chain balances not being immediately evident

The User's position does not necessarily correspond to a balance that can be immediately verified on a single personal *blockchain* address.

Measures in place – the Company ensures that the User's position is tracked by name within its systems; it reconciles the balances recorded in the User's favour with the total balances held; it guarantees the User the ability to view their balances via the Platform and the relevant reporting.

Risk of delays or operational restrictions

Certain transactions, in particular deposits and withdrawals, may be subject to processing times, security checks, internal audits, the number of confirmations required on *the blockchain*, or transfers between hot wallets and cold wallets.

Controls in place – the Company follows formalised operational procedures; carries out preventive checks on withdrawals; uses continuous monitoring systems; and has processes in place for *the escalation* and management of operational incidents.

Residual cyber risk on hot wallets

As Hot Wallets are connected to the operational infrastructure, they present a higher residual cyber risk than Cold Wallets. This risk may relate, for example, to unauthorised access, technical compromises or other cyber security incidents that could result in the loss of the crypto-assets held in custody.

Measures adopted – as extensively described, the Company limits the funds held in hot wallets; applies strong authentication measures; implements controls on access and withdrawals; uses *whitelisting* mechanisms for authorised addresses; continuously monitors operations; and maintains *logging*, incident management and security incident response systems.

Risk of incorrect segregation from the Company's assets

Although the omnibus wallet model does not, in itself, imply a legal commingling of clients' crypto-assets with the Company's assets, there remains a risk that any errors in the configuration of *wallets*, internal records or accounting processes could affect the proper separation between clients' *assets* and the Company's own *assets*. This risk is particularly significant in extreme scenarios, such as insolvency, insolvency proceedings, investigations by third parties or disputes over the ownership of crypto-assets.

Measures in place – The Company ensures that users' crypto-assets and funds are segregated from the Company's assets, through dedicated user *wallets* and accounts, registered in users' names, and separate accounting records attesting to users' rights. In the event of insolvency, users' crypto-assets and funds remain at the disposal of their rightful owners and are returned to the entitled parties on the basis of the Position Register and the relevant records.

Risk of error when executing transfers from Omnibus Wallets

The use of Omnibus Wallets means that outgoing transactions are technically executed from shared *wallets*. In this context, an error in the selection *of the asset*, the amount, the *blockchain*, the destination address or the User's internal position could result in a transfer being executed that is inconsistent with the instruction received. Given the irreversibility of transactions on DLT, the error may not be rectifiable once the transaction has been validated on *the blockchain*.

Measures in place – The Company carries out preliminary checks on transfer instructions, aimed at verifying the completeness of the data, the availability of the crypto-assets, the consistency of the instruction with internal procedures, and the existence of any grounds for refusal or suspension. The transfer *policy* stipulates that the User must provide the data required for the transaction, such as *the wallet address*, amount and type of crypto-asset, and that the Company may reject the instruction in the event of missing or invalid data, insufficient availability, security reasons or cases provided for by anti-money laundering legislation. The Company implements specific operational measures to prevent errors in the execution of transfers from Omnibus Wallets.

Risk of dependence on the correct management of private keys

In the Omnibus Wallet model, the loss, compromise, unavailability or mismanagement of private keys may affect not only a single individual position, but all crypto-assets held in *the wallet* concerned. This risk is significant because the private key constitutes the essential technical means of accessing the custodied crypto-assets.

Measures adopted – The Company uses custody solutions based on distributed signature mechanisms and multi-signature/MPC systems, ensuring that no single party independently holds the entire private key or the *quorum* required to unilaterally transfer the crypto-assets. The architecture is based on *key shares* allocated partly to the technology *provider's* secure infrastructure and partly to Cryptosmart's infrastructure; a *backup* and recovery package for cryptographic keys is available for scenarios where this is required.