ПОЛИТИКА За ПОПЕЧИТЕЛСТВО И АДМИНИСТРИРАНЕ НА КРИПТОАКТИВИ ОТ ИМЕТО НА КЛИЕНТИ	POLICY For CUSTODY AND ADMINISTRATION OF CRYPTO-ASSETS ON BEHALF OF CLIENTS
I. ОБХВАТ И ЦЕЛИ НА ПОЛИТИКАТА. ОБЩИ ПРИНЦИПИ	**I. SCOPE AND GOALS OF THE POLICY. GENERAL PRINCIPLES**
1. Обхват 1.1. Тази политика се прилага за услугите по попечителство и администриране, предоставяни от Сторд Асетс ЕООД, наричано по-долу „Дружеството“. Такива услуги се предоставят независимо или заедно с други услуги, например изпълнение на нареждания или обмен. 1.2. Клиентът може да използва услугите за съхранение и администриране на Дружеството като част от по-голям пакет услуги или отделно – независимо от това, тази политика се прилага за всички услуги, свързани със съхранението и контрола на криптоактиви, предоставяни от клиента, включително под формата на частни криптографски ключове, дори ако Дружеството не може да упражнява права независимо от клиента или трети страни. 1.3. Правно основание и свързани нормативни актове: 1.3.1. Регламент (ЕС) 2023/1114 на Европейския парламент и на Съвета от 31 май 2023 година относно пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на директиви 2013/36/ЕС и (ЕС) 2019/1937 1.3.2. Делегиран регламент (ЕС) 2025/305 на Комисията от 31 октомври 2024 година за допълнение на Регламент (ЕС) 2023/1114 на Европейския парламент и на	**1. Scope** 1.1. This policy is applied to the custody and administration services, provided by Stored Assets LLC, hereinafter referred to as “the Company”. Such services may be provided independently or together with other services, such as the execution of orders and exchange. 1.2. A client may use the custody and administration services of the Company as a part of a larger service package or separately – regardless this policy applies to all services related to safekeeping and controlling of crypto-assets, provided by the client, including in the form of private cryptographic keys, even if the Company cannot exercise rights independently from the client or third parties. 1.3. Legal grounds and related legislation 1.3.1. Regulation (EU) 2023/1114 of the 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 1.3.2. Commission Delegated Regulation (EU) 2025/305 of 31 October 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council

Съвета по отношение на регулаторните технически стандарти за определяне на информацията, която трябва да бъде включена в заявлението за издаване на лиценз за доставчик на услуги за криптоактиви	with regard to regulatory technical standards specifying the information to be included in an application for authorisation as a crypto-asset service provider
1.3.3. Закон за пазарите на криптоактиви	1.3.3. Law on the Markets in Crypto-Assets
1.3.4. Закон за мерките срещу изпиране на пари	1.3.4. Law on the Measures against Money Laundering
1.4. Тази политика ще бъде подлагана на преглед всяка година, както и при установени проблеми, свързани с услугите по попечителство и администриране, предоставяни от Дружеството, съответно при промени в регулаторната рамка.	1.4. This policy shall be subject to **periodic review every year,** as well as in case of established problems related to custody and administration services of the Company, respectively changes in the regulatory framework.
1.5. Тази политика може да бъде изменяна от Изпълнителен директорния орган на Дружеството и измененията влизат в сила от датата на приемането им от Изпълнителен директорния орган.	1.5. This policy may be amended by the management body of the Company and the amendments enter into effect as of the date of their adoption by the management body.
2. Цели на политика	**2. Goals of the Policy**
2.1. Целта на настоящата политика е да създаде ясна рамка за услугите по попечителство и администриране, предоставяни от Дружеството във връзка с криптоактиви от името на клиенти.	2.1. The purpose of the current Policy is to set a clear framework for the custody and administration services provided by the Company with regard to crypto-assets on behalf of clients.
2.2. Политиката гарантира, че Дружеството ще предприема **необходимите стъпки за съхраняване на криптоактиви, предоставени от клиенти, които ще бъдат държавни в нарочен портфейл/сметка за клиентски криптоактиви, отделно от криптоактивите на Дружеството.**	2.2. The Policy guarantees that the Company shall undertake the **necessary steps for safekeeping of crypto-assets provided by clients, which will be held in a dedicated wallet/account for client crypto-assets, separately from the crypto-assets of the Company.**
2.3. Тази политика предвижда допълнителни мерки за уведомяване на клиентите във връзка с права, които те имат във връзка с криптоактивите под попечителството на Дружеството.	2.3. The Policy provides further measures for notifying clients concerning any rights they have with regard to crypto-assets under the Company’s custody.
3. Общи принципи	**3. General principles**
3.1. Точно и своевременно изпълнение на нарежданията на клиенти.	3.1. Exact and timely execution of client orders.

3.2. Стриктно съхраняване на клиентските криптоактиви. 3.3. Своевременно предоставяне на информация до клиента за неговите права във връзка с криптоактивите под попечителство. 3.4. Стриктно отделяне на клиентските активи.	3.2. Strict safekeeping of client assets. 3.3. Timely provision of information to the client with regard to their rights in relation to crypto-assets under custody. 3.4. Strict separation of client assets.
II. ВИД УСЛУГИ ПО ПОПЕЧИТЕЛСТВО И АДМИНИСТРИРАНЕ. СЪОТВЕТНИ МЕРКИ	**II. TYPE OF CUSTODY AND ADMINISTRATION SERVICES. CORRESPONDING MEASURES**
4. Вид услуги по попечителство и администриране 4.1. Дружеството предлага само един стандартен модел на услуга по попечителство и администриране във връзка с криптоактиви, държани от името на клиенти. 4.1.1. Услугата по попечителство и администриране се предоставя чрез мобилното приложение Simple App и се урежда от договора с клиента / Условията за ползване (Terms of Use) и настоящата Политика. 4.1.2. Позоваванията в настоящата Политика на горещи портфейли (hot wallets), студени портфейли (cold wallets), сегрегирани блокчейн адреси (segregated blockchain addresses), омнихус инфраструктура (omnibus infrastructure), вътрешни регистри (internal ledgers) или други технически механизми за съхранение описват вътрешната архитектура за защита на активите (safeguarding architecture), използвана от Дружеството, и не представляват отделни видове клиентски портфейли за попечителство или отделни категории услуги по попечителство и администриране. 4.1.3. В рамките на услугата по попечителство и администриране	**4. Types of custody and administration services** 4.1. The Company offers one standard custody and administration service model only in relation to crypto-assets held on behalf of clients. 4.1.1. The custody and administration service is provided through the Simple App mobile application and is governed by the client agreement / Terms of Use and the present Policy. 4.1.2. References in this Policy to hot wallets, cold wallets, segregated blockchain addresses, omnibus infrastructure, internal ledgers, or other technical storage arrangements describe the internal safeguarding architecture used by the Company and do not constitute separate client-facing custody wallet types or separate categories of custody and administration services. 4.1.3. Under the custody and administration service, the client deposits crypto-assets, or acquires crypto-assets through the Company’s

клиентът депозира криптоактиви или придобива криптоактиви чрез услугите на Дружеството, като тези криптоактиви се отчитат и съхраняват от Дружеството.	services, and such crypto-assets are recorded and safeguarded by the Company.
4.1.4. Клиентските криптоактиви се държат отделно от собствените криптоактиви на Дружеството и се идентифицират във вътрешните регистри и инфраструктурата за съхранение на Дружеството като клиентски активи.	4.1.4. Client crypto-assets are held separately from the Company's own crypto-assets and are identified in the Company's internal records and safeguarding infrastructure as client assets.
4.1.5. Клиентът може да изтегли своите криптоактиви по всяко време, при спазване на приложимите процедури на Дружеството за сигурност, превенция на изпирането на пари и финансирането на тероризма (AML/CFT), санкционен контрол и верификация на трансфери.	4.1.5. The client may withdraw their crypto-assets at any time, subject to the applicable security, AML/CFT, sanctions, and transfer verification procedures of the Company.
4.1.6. Ако възникнат права във връзка с държаните под попечителство криптоактиви, Дружеството уведомява клиента, доколкото това е разумно възможно, за съществуването на тези права и за приложимата процедура за тяхното упражняване.	4.1.6. If rights arise in relation to crypto-assets held in custody, the Company shall notify the client, insofar as reasonably possible, of the existence of such rights and of the applicable procedure for the exercise of such rights.
4.1.7. Дружеството не предлага различни продукти за портфейли за попечителство на различни категории клиенти. Всички оперативни, технически или специфични за даден актив механизми, използвани от Дружеството, са част от един и същ единен модел на услуга по попечителство и администриране.	4.1.7. The Company does not offer different custody wallet products to different categories of clients. Any operational, technical, or asset-specific arrangements used by the Company form part of the same single custody and administration service model.
4А. Оперативни и ИКТ механизми за попечителство и администриране	**4A. Operational and ICT arrangements for custody and administration**
4А.1. Услугата по попечителство и администриране се поддържа от оперативна и ИКТ рамка, предназначена да защитава клиентските криптоактиви и средствата за достъп до тях срещу загуба, кражба, неправомерно използване, неразрешен трансфер, вътрешни измами, кибератаки, човешка грешка, технологичен отказ и прекъсване на услуги от трети страни.	4A.1. The custody and administration service is supported by an operational and ICT framework designed to safeguard client crypto-assets and the means of access thereto against loss, theft, misuse, unauthorized transfer, internal fraud, cyber-attack, human error, technology failure, and third-party service disruption.

4А.2. Дружеството използва технология за многостранно изчисление (Multi-Party Computation – MPC) и ролево-базирани оперативни контроли, така че нито едно лице или система самостоятелно да не може да контролира или прехвърля клиентски криптоактиви извън одобрения процес за авторизация.	4A.2. The Company uses Multi-Party Computation (MPC) technology and role-based operational controls so that no single individual or system can unilaterally control or transfer client crypto-assets outside the approved authorization workflow.
4А.3. Достъпът до системите, свързани с попечителството, е ограничен до надлежно оправомощен персонал на принципа "необходимост да се знае" и е защитен чрез силна автентикация, процеси на одобрение, водене на системни записи и непрекъснат мониторинг.	4A.3. Access to custody-related systems is restricted to duly authorized personnel on a need-to-know basis and is protected by strong authentication, approval workflows, logging, and ongoing monitoring.
4А.4. Дружеството прилага правила за авторизация на трансакции, включително изисквания за одобрение от множество лица при съществени или чувствителни операции, както и оперативни прагове, контроли за равняване и процедури за ескалация при необичайни събития.	4A.4. The Company applies transaction authorization rules, including multi-person approval requirements for material or sensitive operations, as well as operational thresholds, reconciliation controls, and escalation procedures for irregular events.
4А.5. Дружеството поддържа механизми за архивиране и възстановяване на данни, включително мерки за възстановяване при бедствия, предназначени да осигурят непрекъснатост на защитата и възможност за възстановяване на клиентските криптоактиви в случай на отказ на доставчик, техническа неизправност или друго сериозно прекъсване.	4A.5. The Company maintains backup and recovery arrangements, including disaster recovery measures intended to ensure continuity of safeguarding and the recoverability of client crypto-assets in the event of provider failure, technical malfunction, or other severe disruption.
4А.6. Клиентските криптоактиви се идентифицират чрез счетоводните и вътрешните регистри на Дружеството, вътрешния леджър, записите по клиентските сметки и инфраструктурата на портфейлите, включително чрез свързване на съответните адреси на портфейли, баланси на активите и история на трансакциите към съответния клиент.	4A.6. Client crypto-assets are identified through the Company’s books and records, internal ledger, client account records, and wallet infrastructure, including the attribution of relevant wallet addresses, asset balances, and transaction history to the relevant client.
4А.7. Дружеството поддържа регистър на клиентските активи и процедури за равняване, които позволяват бързото	4A.7. The Company maintains a client asset register and reconciliation procedures enabling the prompt identification, segregation, and return of client crypto-assets.

идентифициране, отделяне (сегрегация) и връщане на клиентските криптоактиви.	
4А.8. Дружеството връща клиентските криптоактиви или позволява тяхното прехвърляне към портфейл или сметка, посочени от клиента, в съответствие с приложимите договорни условия, контролите върху трансферите, AML/CFT проверките, санкционния скрининг и мерките за верификация на сигурността.	4A.8. The Company returns client crypto-assets or enables their transfer to a wallet or account designated by the client in accordance with the applicable contractual terms, transfer controls, AML/CFT checks, sanctions screening, and security verification measures.
4А.9. Дружеството прилага процедури за реакция при инциденти, осигуряване на непрекъснатост на дейността и възстановяване при бедствия, с цел минимизиране на риска от загуба на клиентски криптоактиви или на средствата за достъп до тях, както и за възстановяване на критичните операции по попечителство без неоправдано забавяне.	4A.9. The Company has in place procedures for incident response, business continuity, and disaster recovery in order to minimize the risk of loss of client crypto-assets or of the means of access thereto and to restore critical custody operations without undue delay.
4Б. Използване на доставчици на услуги – трети страни	**4B. Use of third-party service providers**
4Б.1. При предоставянето на услугата по попечителство и администриране Дружеството може да използва надлежно подбрани трети страни – доставчици на технологии и инфраструктура, които подпомагат специфични елементи от оперативния модел на попечителство.	4B.1. In providing the custody and administration service, the Company may use duly selected third-party technology and infrastructure providers that support specific elements of the custody operating model.
4Б.2. Използването на такива трети страни доставчици не създава отделен вид портфейл за попечителство или отделна услуга по попечителство за клиентите и представлява част от единния модел на услугата по попечителство и администриране на Дружеството.	4B.2. The use of such third-party providers does not create a separate custody wallet type or a separate custody service for clients and forms part of the Company’s single custody and administration service model.
4Б.3. Когато доставчик – трета страна подпомага защитата на активите, инфраструктурата за управление на криптографски ключове, сигурността на трансакциите, възстановяването при бедствия или друга свързана функционалност по попечителство, Дружеството извършва комплексна проверка, договорен надзор, оценка на	4B.3. Where a third-party provider supports safeguarding, key-management infrastructure, transaction security, disaster recovery, or related custody functionality, the Company shall perform due diligence, contractual oversight, security assessment, and ongoing monitoring of such provider in accordance with the Company’s outsourcing,

сигурността и текущ мониторинг на този доставчик в съответствие с рамката на Дружеството за изнасяне на дейности, управление на ИКТ рисковете и оперативна устойчивост.	ICT risk, and operational resilience framework.
4Б.4. Дружеството остава отговорно за спазването на приложимите регулаторни изисквания във връзка с услугата по попечителство и администриране, включително за защитата на клиентските криптоактиви и правилното функциониране на процедурите за идентификация и връщане на клиентските активи.	4B.4. The Company remains responsible for compliance with the applicable regulatory requirements in relation to the custody and administration service, including the safeguarding of client crypto-assets and the proper operation of client asset identification and return procedures.
4.2. Описание на услугите по попечителство и администриране: 4.2.1. Естество на услугата – клиентът депозира криптоактиви по своя собствена преценка по отделен портфейл/сметка, държани от Дружеството. 4.2.2. Дружеството приема за съхранение и администриране само онези видове криптоактиви, които са изрично изброени в Програмата за дейността на Дружеството, одобрена от компетентния орган. Пълният и изчерпателен списък на поддържаните криптоактиви се поддържа вътрешно от Дружеството и е предоставен на клиентите чрез приложението Simple. Дружеството не приема други криптоактиви за съхранение по силата на отделни или допълнителни споразумения. 4.2.3. Отделният портфейл/сметка се използва само за съхранение на криптоактиви на клиента и се управлява отделно от криптоактивите на Компанията. 4.2.4. Криптоактивите на клиентите се държат отделно в разпределения регистър от криптоактивите на Компанията в съответствие с политиката за разделяне на клиентските средства и клиентските криптоактиви.	4.2. Description of the custody and administration service: 4.2.1. Nature of the service – the client deposits cyrptoassets under their own discretion to a dedicated wallet/account held by the Company. 4.2.2. The Company accepts for custody and administration only those types of crypto-assets that are explicitly listed in the Company's Programme of Operations as approved by the competent authority. The comprehensive and exhaustive list of supported crypto-assets is maintained internally by the Company and is made available to clients via the Simple App. The Company does not accept any other crypto-assets for custody under separate or additional agreements. 4.2.3. The dedicated wallet/account is used only for safekeeping of client crypto-assets and is managed separately from Company crypto-assets. 4.2.4. Client crypto-assets are held separately on the distributed ledger from Company crypto-assets in accordance with the policy for segregation of client funds and client crypto-assets.

4.2.5. Клиентът може да използва функционалностите на мобилното приложение за други услуги на Дружеството или да тегли своите криптоактиви по всяко време в съответствие с приложимите политики на Дружеството.	4.2.5. The client may use the functionalities of the mobile application for other services of the Company or withdraw their crypto-assets at any time in accordance with the applicable policies of the Company.
4.2.6. Дружеството уведомява клиента в случай че за него възникнат права по отношение на криптоактивите, намиращи се под попечителство на Дружеството. В тези случаи правата не могат да бъдат упражнявани от клиентите, докато криптоактивите са под попечителство на Дружеството – клиентът може да изтегли своите криптоактиви и да упражни правата си сам.	4.2.6. The Company notifies the client in case any rights arise for them with regard to the crypto-assets under the Company's custody. In these cases the rights cannot be exercised by the clients while the crypto-assets are under the Company's custody – the client may withdraw their crypto-assets and exercise their rights themselves.
4.2.7. В случай на еърдроп или други подобни събития, свързани с криптоактиви под попечителство на Дружеството, за Дружеството възникват всички ползи.	4.2.7. In case of airdrop or other such events, related to crypto-assets under the Company's custody, any benefits arise for the Company.
4.2.8. Дружеството не предлага различни видове услуги по попечителство и администриране. Всякакви специфични за клиента договорни разпоредби, когато са допустими, не променят единния модел на услугата по попечителство и администриране, описан в настоящата Политика.	4.2.8. The Company does not offer different types of custody and administration services. Any client-specific contractual provisions, where permitted, shall not alter the single custody and administration service model described in this Policy.
5. Съотношение с други вътрешни документи на Дружеството	**5. Relation to other internal documents of the Company**
5.1. Правилата за получаване и изпълнение на клиентски нареждания, включително за администриране на клиентски активи, както и правилата за комуникация с клиента, се съдържат в Политиката за изпълнение на клиентски нареждания.	5.1. The rules for receipt and execution of client orders, including for administration of client assets, as well as the rules for communication with the client, are contained in the Policy for execution of client orders.
5.2. Правилата за приемане, отделяне и връщане на клиентски активи се съдържат в Процедурата за отделяне на клиентски средства и криптоактиви.	5.2. The rules for acceptance, separation and return of client assets are contained in the Procedure for separation of client funds and crypto-assets.
5.3. Правилата за предотвратяване на изпирането на пари са определени в	5.3. The rules for prevention of money-laundering are set in the Policy for prevention

Политиката за предотвратяване на изпирането на пари. 5.4. Правилата за управление на оперативните рискове и цифрова устойчивост са закрепени в Политиката за управление на ИКТ рисковете и рисковете за сигурността (DORA мерки)	of money laundering. 5.4. The framework for operational risk management and digital resilience is set in the ICT & Security Risk Management Policy (DORA Framework).
III. ЛИЦА, ОТГОВОРНИ ЗА СПАЗВАНЕ НА ТАЗИ ПОЛИТИКА	**III. PERSONS RESPONSIBLE FOR COMPLIANCE WITH THIS POLICY**
6. Изпълнителен директор (Съответствие и риск) 6.1. Изпълнителният директор (Съответствие и риск) е отговорен за въвеждането и спазването на настоящата Политика. 6.2. Изпълнителният директор (Съответствие и риск) издава задължителни инструкции относно прилагането на настоящата Политика. 6.3. Изпълнителният директор (Съответствие и риск) може да изисква информация и справки относно услугите по пазене и администриране, предоставяни от Дружеството. 6.4. Изпълнителният директор организира периодични и извънредни обучения и тестове относно прилагането на настоящата Политика. 6.5. Изпълнителният директор (Съответствие и риск) може да предприема всякакви други мерки, за да гарантира спазването на настоящата Политика. 6.6. Изпълнителният директор (Съответствие и риск) има право да получава отчети от всички други отговорни лица в съответствие с настоящата процедура и може лично да проверява операциите и Регистъра на позициите по настоящата Политика. 6.7. Изпълнителният директор (Съответствие и риск) е отговорен за координацията между всички други лица,	**6. Executive Director** (Compliance & Risk) 6.1. The Executive Director (Compliance & Risk) is responsible for the introduction and compliance with this Policy. 6.2. The Executive Director (Compliance & Risk) issues mandatory instructions concerning the application of this Policy. 6.3. The Executive Director (Compliance & Risk) can require information and references concerning the custody and administration services, provided by the Company. 6.4. The Executive Director (Compliance & Risk) organizes periodical and emergency training and tests concerning the application of this Policy. 6.5. The Executive Director (Compliance & Risk) can undertake any other measures to guarantee the compliance with this procedure. 6.6. The Executive Director (Compliance & Risk) has the right to receive reports by all other responsible persons in accordance with this procedure and can personally inspect the operations and the Register of positions under this Policy. 6.7. The Executive Director (Compliance & Risk) is responsible for the coordination between all other persons who have obligations under this Policy.

които имат задължения по настоящата Политика. 6.8. За целите на настоящата политика, Изпълнителният директор (Съответствие и риск) за регулаторен надзор е изпълнителният директор, отговарящ за съответствието.	6.8. For the purposes of this Policy, the Executive Director (Compliance & Risk) responsible for regulatory oversight is designated as the Chief Compliance Officer (CCO).
7. Изпълнителният директор, отговарящ за съответствието 7.1. Изпълнителният директор, отговарящ за съответствието е надлежно назначен служител, който преглежда спазването на регулаторната рамка и вътрешните процедури на Дружеството. 7.2. Изпълнителният директор, отговарящ за съответствието е длъжен да извършва периодични и извънредни проверки за спазване на настоящата Политика. 7.3. Изпълнителният директор, отговарящ за съответствието може да изисква справки и информация, както и лично да проверява операциите и Регистъра на позициите по настоящата Политика. 7.4. Изпълнителният директор, отговарящ за съответствието е длъжен незабавно да уведомява Изпълнителния директор при установени нередности. 7.5. Изпълнителният директор, отговарящ за съответствието е длъжен незабавно да прекратява операции, несъответстващи на настоящата Политика, и да издаде указания за спазване на настоящата Политика при установени нередности. 7.6. Изпълнителният директор, отговарящ за съответствието е длъжен да предоставя на Изпълнителния директор отчет на всеки 3 месеца относно извършените проверки и установените обстоятелства, заедно с препоръки за предотвратяване на рискове в обхвата на настоящата Политика.	7. **Chief Compliance Officer (CCO)** 7.1. The Chief Compliance Officer (CCO) is a duly appointed employee, who reviews the compliance with the regulatory framework and the internal procedures of the Company. 7.2. The Chief Compliance Officer (CCO) is obliged to perform periodical and emergency audits for the compliance with the current Policy. 7.3. The Chief Compliance Officer (CCO) may require references and information, as well as personally inspect the operations and the Register of positions under this Policy. 7.4. The Chief Compliance Officer (CCO) is obliged to immediately notify the Executive Director in the event of established irregularities. 7.5. The Chief Compliance Officer (CCO) is obliged to immediately cease operations non-compliant with this Policy and to issue instructions for compliance with the current Policy in the event of established irregularities. 7.6. The Chief Compliance Officer (CCO) is obliged to provide a report to the Executive Director every 3 months concerning the conducted audits and the established circumstance, along with recommendations for preventing risks in the scope of this Policy.

7.7. Изпълнителният директор, отговарящ за съответствието е длъжен да спазва указанията и разпорежданията на Изпълнителния директор по отношение на спазването на настоящата Политика.	7.7. The Chief Compliance Officer (CCO) is obliged to follow the instructions and orders of the Executive Director with regard to the compliance with this Policy.
8. Изпълнителен директор (Операции и технологии) 8.1. Изпълнителен директор (Операции и технологии) е отговорен за прилагането на мерките за съхранение и администриране на клиентските активи. 8.2. Изпълнителен директор (Операции и технологии) е длъжен да извършва периодични и извънредни проверки на използваните технически средства и мерки за услуги по съхранение и администриране. 8.3. Изпълнителен директор (Операции и технологии) е длъжен да уведоми незабавно Изпълнителния директор при установени нередности. 8.4. Изпълнителен директор (Операции и технологии) има право да издава задължителни указания относно спазването на настоящата Политика, както и да предлага на Изпълнителния директор изменения в нея. 8.5. Изпълнителен директор (Операции и технологии) е длъжен да предоставя на Изпълнителния директор отчет за извършените проверки и установените обстоятелства, заедно с препоръки за предотвратяване на рискове в обхвата на настоящата Политика, на всеки 3 месеца. 8.6. Изпълнителен директор (Операции и технологии) е длъжен да спазва указанията и разпорежданията на Изпълнителния директор относно спазването на настоящата Политика.	**8. Executive Director (Operations & Technology)** 8.1. The Executive Director (Operations & Technology) is responsible for the implementation of the measures for custody and administration of client assets. 8.2. The Executive Director (Operations & Technology) is obliged to conduct periodic and emergency checks of the used technical devices and measures for custody and administration services. 8.3. The Executive Director (Operations & Technology) is obliged to notify immediately the Executive Director in case of established irregularities. 8.4. The Executive Director (Operations & Technology) has the right to issue mandatory instructions with regard to the compliance with this Policy, as well as suggest amendments thereto to the Executive Director. 8.5. The Executive Director (Operations & Technology) is obliged to provide a report to the Executive Director for the performed checks and the established circumstances, along with recommendations for prevention of risks in the scope of the current Policy, every 3 months 8.6. The Executive Director (Operations & Technology) is obliged to follow the instructions and orders of the Executive Director with regard to the compliance with this Policy.
9. Ръководител на операциите 9.1. Ръководител на операциите следи за спазването на правилата на настоящата	**9. Head of Operations** 9.1. The Head of Operations Department monitors the compliance with the rules of the

Политика от всички служители на Отдел „Операции”.	current Policy by all employees of the Operations Department.
9.2. Ръководител на операциите осъществява оперативно ръководство на всички служители на Отдел „Операции”.	9.2. The Head of Operations Department performs operative management of all employees of the Operations Department.
9.3. Ръководител на операциите осъществява постоянен контрол върху операциите, свързани с попечителските и административните услуги, включително регистрацията на данни в Регистъра на позициите.	9.3. The Head of Operations Department performs constant control over the operations related to custody and administration services. including the registration of data in the Register of positions.
9.4. Ръководител на операциите уведомява незабавно Изпълнителния директор и вътрешния контрол при установени нередности.	9.4. The Head of Operations Department notifies immediately the Executive Director and the Chief Compliance Officer (CCO) in case of established irregularities.
9.5. Ръководител на операциите организира периодични обучения на служителите в Отдел „Операции”.	9.5. The Head of Operations Department organizes periodic trainings of the employees in the Operations Department.
9.6. Ръководител на операциите одобрява следните операции преди тяхното извършване:	9.6. The Head of Operations Department approves the following operations before their performance:
9.6.1. Всички изходящи прехвърляния, надхвърлящи автоматичен праг от 50 000 евро (или еквивалента им).	9.6.1. All outgoing crypto-asset transfers exceeding the automated threshold of €50,000 (or equivalent).
9.6.2. Техническата конфигурация или въвеждането на нова блокчейн мрежа или стандарт за токени в средата за попечителство.	9.6.2. The technical configuration and enabling of any new blockchain network or token standard within the custody environment.
9.6.3. Всяко ръчно засичане на наличностите или коригиране на баланса в резултат на докладван системен инцидент или техническа малфункция	9.6.3. Any manual reconciliation or balance adjustment resulting from a reported system incident or technical failure.
9.7. Ръководител на операциите предоставя отчет на Изпълнителния директор относно попечителските и административните услуги всеки месец.	9.7. The Head of Operations Department provides a report to the Executive Director concerning the custody and administration services each month.
9.8. Ръководител на операциите може да изисква информация и препоръки от служителите в Отдел „Операции”.	9.8. The Head of Operations Department can require information and references from the employees in the Operations Department.
9.9. Ръководител на операциите е длъжен да следва инструкциите на Изпълнителния директор, вътрешния контрол и Ръководителя на техническия	9.9. The Head of Operations Department is obliged to follow the instructions of the Executive Director, the Chief Compliance Officer (CCO) and the Executive Director

отдел по отношение на услугите по съхранение и администриране. 9.10. Ръководител на операциите извършва периодични и извънредни проверки за съответствието на услугите по съхранение и администриране с настоящата Политика.	(Operations & Technology) with regard to the custody and administration services. 9.10. The Head of Operations Department performs periodic and emergency checks of the compliance of the custody and administration services with this Policy.
10. Отдел „Операции” 10.1. Служителите от Отдел „Операции” носят отговорност за съответствието на действията си с разпоредбите на настоящата Политика. 10.2. Служителите от Отдел „Операции” предоставят информация на клиентите относно услугите по попечителство и администриране, предоставяни от Дружеството. 10.3. Услугата по попечителство и администриране, предоставяна от Дружеството, се урежда от Общите условия и настоящата Политика. 10.4. Служителите от Отдел „Операции” предприемат необходимите действия съгласно настоящата Политика и стриктно спазват договорите с всеки клиент. 10.5. Служителите от Отдел „Операции” уведомяват клиента преди да предприемат каквито и да е действия по попечителство или управление, освен ако договорът с клиента не предвижда друго. 10.6. Служителите от Отдел „Операции” винаги предоставят информация на клиента за действията по съответната услуга по попечителство или административно обслужване. 10.7. Служителите от Отдел „Операции” въвеждат необходимите данни съгласно настоящата Политика в Регистъра на позициите. 10.8. Служителите от Отдел „Операции” стриктно спазват правилата за документиране на клиентските поръчки.	**10. Operations Department** 10.1. The employees from Operations Department are responsible for the compliance of their actions with the provisions of this Policy. 10.2. The employees from Operations Department provide information to clients about the custody and administration services, provided by the Company. 10.3. The custody and administration service provided by the Company is governed by the Terms of Conditions and the present Policy. 10.4. The employees from Operations Department undertake the necessary actions as per this Policy and strictly observe the contracts with each client. 10.5. The employees from Operations Department notify the client before undertaking any action for custody or management, unless the contract with the client stipulates otherwise. 10.6. The employees from Operations Department always provide information to the client about the actions under the custody or administrative service. 10.7. The employees from Operations Department enter the necessary data as per this Policy in the Register of positions. 10.8. The employees from Operations Department strictly follow the rules for documenting the client’s orders.

10.9. Служителите от Отдел „Операции” стриктно спазват правилата за разделяне на клиентските средства и активи. 10.10. Служителите от Отдел „Операции” спазват процедурата за проверка на клиентските поръчки и изискват одобрение на съответното действие от началника на Отдел „Операции” в следните случаи: 10.10.1. Всяко действие за размразяване на клиентски портфейл или сметка след замразяването му по съображения за сигирност или в съответствие с политиката за мерките срещу изпиране на пари се одобрява от началника на отдел „Операции” или Изпълнителният директор, отговарящ за съответствието 10.10.2. Всяко ръчно настройване на клиентски баланс (напр. поради технически грешки или връщане на средства) на стойност над 1 000 евро. 10.10.3. Посочване на нов адрес към белия списък на Дрижеството за оперативни прехвърляния. 10.11. Служителите от отдел „Операции“ стриктно спазват инструкциите на изпълнителния директор (Операции и технологии), главния директор по съответствие (CCO), изпълнителния директор (Операции и технологии) и ръководителя на „Операции“.	10.9. The employees from Operations Department strictly follow the rules for separation of client fund and assets. 10.10. The employees from Operations Department follow the procedure for verifying client orders and require approval of the respective action by the Chief of the Operations Department in the following cases: 10.10.1. Any action to unfreeze a client's wallet or account after a security lockdown or AML suspension requires is to be approved by the Head of Operations or the Chief Compliance Officer (CCO) 10.10.2. Any manual adjustment to client balances (e.g., due to technical errors or refunds) exceeding €1,000 in value. 10.10.3. Adding a new destination address to the Company’s corporate whitelist for operational transfers. 10.11. The employees from Operations Department strictly follow the instructions of the Executive Director (Operations & Technology), the Chief Compliance Officer (CCO), the Executive Director (Operations & Technology) and the Head of Operations.
IV. ПРОЦЕДУРИ ЗА ПРЕДОСТАВЯНЕ НА УСЛУГИ ПО ПОПЕЧИТЕЛСТВО И АДМИНИСТРИРАНЕ	**IV. PROCEDURES FOR PROVIDING CUSTODY AND ADMINISTRATION SERVICES**
11. Общи разпоредби 11.1. Услугите по попечителство и администриране се предоставят въз основа на договор с клиента. Договорът съдържа най-малко следните клаузи: 11.1.1. Идентификация на страните. 11.1.2. Характер на предоставяната услуга и нейното описание.	**11. General provisions** 11.1. Custody and administration services are provided on basis of a contract with the client. The contract contains at least the following clauses: 11.1.1. Identification of the parties. 11.1.2. The nature of the service provided and a description thereof.

11.1.3. Настоящата политика за попечителство.	11.1.3. The current policy for custody.
11.1.4. Средства за комуникация между Дружеството и клиента, включително средства за удостоверяване на клиента – в съответствие с политиката за изпълнение на нареждания.	11.1.4. The means of communication between the Company and the client, including the means for authentication of the client – in compliance with the policy for execution of orders.
11.1.5. Изрична уговорка, че всякакви права във връзка с криптоактивите под попечителство може да се упражняват само след като клиентът изтегли тези криптоактиви по портфейл / сметка под свой контрол	11.1.5. Explicit clause that any rights with regard to crypto-assets under custody may be exercised only after the client withdraws the crypto-assets to wallet/account under the client's control.
11.1.6. Изрична клауза, че всякакви криптоактиви разпределени от мрежата или издателя на криптоактива във връзка с криптоактиви по портфейла / сметката на Дружеството остават собственост на Дружеството	11.1.6. Explicit clause that any crypto-assets allocated by the DLT network or crypto-asset issuer with regard to crypto-assets in the client wallet/account of the Company remain for the Company.
11.1.7. Описание на системите за сигурност на Дружеството.	11.1.7. A description of the security systems of the Company.
11.1.8. Такси, разходи и разноски, прилагани от Дружеството.	11.1.8. The fees, costs and charges applied by the Company.
11.1.9. Приложимото право към договора.	11.1.9. The law applicable to the contract.
11.1.10. Клауза за юрисдикция, определяща съдилищата на коя държава могат да разрешават спорове, произтичащи от или свързани с договора	11.1.10. Jurisdiction clause determining the courts of which country can resolve disputes arising from or related to the contract.
11.2. Цялата комуникация с клиента – нареждания, уведомления и др. – се осъществява по каналите, посочени в договора към всеки договор, и в съответствие с правилата за изпълнение на клиентски нареждания.	11.2. All communication with the client – orders, notifications, etc. – shall be conducted via the channels specified in the contract with each contract and in compliance with the rules for executing client orders.
11.3. Дружеството предоставя услугите по попечителство и администриране за срока на договора и връща криптоактивите на клиента съгласно процедурата за разделяне на клиентските средства.	11.3. The Company provides the custody and administration services for the duration of the contract and returns the crypto-assets to the client in accordance with the procedure for separation of client funds.
11.4. Клиентът може да поиска криптоактивите да бъдат върнати в по-ранен момент по негова преценка.	11.4. The client can require the crypto-assets to be returned at an earlier moment upon his discretion.
11.5. Служител от Отдел „Операции" уведомява клиента 14 дни преди изтичане	11.5. An employee from Operations Department shall notify the client 14 days

на договора за попечителство и администриране. След изтичане на срока на договора клиентът следва да заяви как желае да получи поставените под попечителство криптоактиви или да удължи договора – при същите или различни условия.	before the expiry of the contract for custody and administration service. Upon expiry the client shall indicate how they prefer to receive the crypto-assets under custody or extend the contract – under the same or different terms.
11.6. След изтичане на договор за услуга по съхранение и администриране, ако клиентът не е потърсил връшане на своите криптоактиви, Дружеството продължава да съхранява тези криптоактиви. Клиентът се таксува за услугата за попечителство и всички дължими такси могат да бъдат събрани от неговите средства и активи, предоставени на Дружеството, в съответствие с политиката за такси и разходи.	11.6. After expiry of a contract for custody and administration service, if the client has not required their crypto-assets to be returned the Company continues to store these crypto-assets. The client shall be charged for the custody service and any due fees can be collected from the client's funds and assets in line with the policy for fees and expenses.
11.7. Служителите от Отдел „Операции" предоставят резюме на тази политика на клиентите при поискване.	11.7. The employees from the Operations Department provide a summary of this policy to clients upon request.
11.8. Дружеството носи отговорност пред клиентите за загубата на криптоактиви или средствата за достъп до тях, когато загубата е настъпила по вина на Дружеството или в резултат на технически проблем или кибер-атака. Отговорноста на Дружеството е ограничена до пазарната стойност на криптоактивите към момента на загубата им.	11.8. The Company is liable to its clients for the loss of any crypto-assets or of the means of access to the crypto-assets as a result of an incident that is attributable to the Company or as a result of a malfunction or a cyber-attack. The liability of the Company is capped at the market value of the crypto-assets lost at the time the loss occurred.
11.9. Дружеството не носи отговорност за загуби, причинени от инцидент, възникнал независимо от предоставената услуга или поради обстоятелства, които са извън контрола на Дружеството.	11.9. The Company is not liable for loss due to incident that has occurred independent of the provided service or due to circumstances which are outside of the Company's control.
11.10. В договора страните могат да се споразумеят, че Дружеството ще използва услугите на трети страни за предоставяне на част от услугите. В тези случаи Дружеството възлага такива услуги само след предварително уведомяване на клиента и само на доставчици на услуги, които са надлежно лицензирани в съответствие със законодателството на ЕС	11.10. In the contract the parties can agree that the Company shall use the services of third parties for providing a part of the services. In these cases the Company shall assign such services only after prior notification of the client and only to service-providers who are duly licensed in accordance

и по-специално с Регламент (ЕС) 2023/1114.	with EU legislation and Regulation (EU) 2023/1114 in specific.
12. Отговорност за загуба на криптоактиви	**12. Liability for loss of crypto-assets**
12.1. В съответствие с чл. 75, параграф 8 от Регламент (ЕС) 2023/1114 (MiCA), Дружеството носи отговорност пред своите клиенти за загубата на криптоактиви или на средствата за достъп до криптоактиви, държани под попечителство, в резултат на инцидент, за който Дружеството или трета страна – доставчик на услуги, на която са възложени функции по попечителство, носи отговорност.	12.1. In accordance with Article 75(8) of Regulation (EU) 2023/1114 (MiCA), the Company shall be held liable to its clients for the loss of any crypto-assets or of the means of access to the crypto-assets held in custody as a result of an incident that is attributable to the Company or to a third-party service provider to which custody functions have been outsourced.
12.2. Тази отговорност покрива загуби, произтичащи от свързани с ИКТ инциденти, включително инциденти в резултат на кибератака, кражба или всякаква неизправност на системите, използвани или контролирани от Дружеството.	12.2. Such liability covers losses resulting from ICT-related incidents, including incidents resulting from a cyber-attack, theft, or any malfunction of the systems used or controlled by the Company.
12.3. Отговорността на Дружеството е ограничена до пазарната стойност на изгубените криптоактиви към момента на настъпване на загубата.	12.3. The liability of the Company shall be capped at the market value of the lost crypto-assets at the time the loss occurred.
12.4. Дружеството не носи отговорност за загубата на криптоактиви или средства за достъп, когато може да докаже, че загубата е настъпила в резултат на събитие или обстоятелства извън неговия разумен контрол, чиито последици не биха могли да бъдат избегнати въпреки всички разумни усилия за обратното (напр. присъщи уязвимости в технология на разпределения регистър или протокол без разрешение (permissionless DLT)).	12.4. The Company shall not be liable for the loss of crypto-assets or means of access where it can prove that the loss occurred as a result of an event or circumstances outside of its reasonable control, the consequences of which could not have been avoided despite all reasonable efforts to the contrary (e.g., inherent vulnerabilities in a permissionless distributed ledger or protocol).
12.5. В случай на загуба на криптоактиви или средства за достъп, за които Дружеството носи отговорност, Дружеството възстановява на клиента криптоактиви от същия вид и в същия размер или, когато това не е възможно, обезщетява клиента до размера на	12.5. In the event of a loss of crypto-assets or means of access for which the Company is liable, the Company shall restitute crypto-assets of the same type and in the same amount to the client, or, where this is not possible, compensate the client up to the

пазарната стойност на изгубените криптоактиви към момента на загубата.	market value of the lost crypto-assets at the time of the loss.
13. Права на клиентите във връзка със специфични случаи 13.1. Дружеството предоставя попечителски услуги само във връзка със съхранение на клиентски криптоактиви. Ако криптоактивите предоставят права на клиента, тези права се упражняват само от клиента и само след като клиентът изтегли своите криптоактиви по портфейл/сметка под неговия контрол. 13.2. Дружеството отговаря само за съхранението на клиентските криптоактиви. 13.3. Ако за клиента възникват права, Дружеството ще уведоми клиента, доколкото е възможно, за тези права и ще посочи, че тези права се упражняват само от от клиента и само след като криптоактивите са прехвърлени по портфейл/сметка под контрола на клиента. Това се прилага също в случаи на еърдроп, разделяне на мрежата и други събития, които засягат криптоактивите на клиента. 13.4. За криптоактиви, които остават под попечителството на Дружеството, всякакви последици и промени в наличините криптоактиви не засягат баланса на клиента. Разпределени от мрежата или емитента криптоактиви остават за сметка на Дружеството.	**13. Client rights with regard to specific cases** 13.1. The Company provides only custody services related to safekeeping of client crypto-assets. If the crypto-assets allow any rights to the client, these rights may be exercised only by the client and only if the client withdraws their crypto-assets to a wallet/account under the client's control. 13.2. The Company is responsible only for the safekeeping of the client crytpo-assets. 13.3. If any rights arise for the client, the Company will notify the client, insofar possible, about these rights and will indicate that the rights can be exercised only by the client and only after the crypto-assets have been transferred to a wallet/account under the client's control. This also applies in cases of airdrops, forks and other events affecting the client's crypto-assets. 13.4. For crypto-assets which remain under the Company's custody, any effects and changes to the available crypto-assets do not affect the client's balance. Any crypto-assets allocated under any way by the DLT network or the crypto-asset issuer remain for the Company.
V. РЕГИСТЪР НА ПОЗИЦИИТЕ	**V. REGISTER OF POSITIONS**
14. Изисквания към Регистър на позициите 14.1. Дружестото поддържа Регистр на клиентските позиции, в който се съдържа информация, свързана с предоставяните услуги по попечителство и адмиистриране. 14.2. Регистърът съдържа информация за предоставените от клиента криптоактиви, както следва: 14.2.1. Идентификация на клиента' 14.2.2. Видове криптоактиви	**14. Requirements for the Register of Positions** 14.1. The Company keeps a Register of client positions, containing the information related to the provided custody and administration services. 14.2. The Register contains information about the crypto-assets, provided by the client, as follows: 14.2.1. Identification of the client 14.2.2. Types of crypto-assets

14.2.3. Количество за всеки вид криптоактив 14.2.4. Дата на предоставяне на всеки криптоактив и всяка промяна в количеството 14.2.5. Разпределение между различни портфейли/сметки 14.2.6. Информация за впсиването / индивидуалнат апартида на клиента в счетоводството на Дружеството; 14.2.7. Събития, които засягат криптоактивите 14.2.8. Съития, кото може да доведат до възникване или изменение на правата на клиента 14.2.9. Изпратени до клиента уведомления 14.2.10. Поулчени нареждания от клиента 14.2.11. Действия, изпълнени от Дружеството, включително трансакции, нареждания към трети страни и т.н. 14.2.12. Инциденти, свързрани с криптоактивире под попечителство. 14.3. **Служителите от отдел Клиентски средства отговарят за незабавното актуализиране на вписаните в Регистъра данни.** 14.4. Служителите от отдел Клиентски средства изпращат на клиента справка от Регистъра относно неговите криптоактивите под попечителство или администриране на всеки три месеца, както и при искане от клиента, в срок от 3 дни от получаване на искането.	14.2.3. Amount for each type of crypto-asset 14.2.4. Date of providing each crypto-asset and every change to the amount thereof 14.2.5. Distribution between different wallets/accounts 14.2.6. Information for the entry/personal partition of the client in the accounting of the Company 14.2.7. Events affecting the crypto-assets 14.2.8. Events likely to create or modify the rights of the client 14.2.9. Sent notifications to the client 14.2.10. Orders received from the client 14.2.11. Actions performed by the Company, including transactions, orders to third parties, etc. 14.2.12. Incidents related to the crypto-assets under custody 14.3. **The employees from the Operations Department are responsible for immediately updating the entries in the Register.** 14.4. The employees from the Operations Department send to the client an excerpt from the Register concerning the client's crypto-assets under custody or administration every 3 months, as well as upon request from the client, within 3 days from the request.
15. **Съгласуване със счетоводни регистри** 15.1. Служителите от отдел Клиентски средства изпращат информация към Отдел Счетоводство във връзка с всяка промяна в клиентските активи в съответствие с политиката за отделяне на клиентски средства и активи. 15.2. Служителите от отдел Клиентски средства съгласуват периодично	**15. Coordination with accounting registries** 15.1. The employees from the Operations Department send information to the Accounting Department concerning any change in the amounts of client crypto-assets in accordance with the policy for separation of client funds and assets. 15.2. The employees from the Operations Department coordinate the amounts of client

количествата клиентски активи по всяка позиция в Регистър на позициите с отдел Счетоводство и преди всяка операция в съответствие с политиката за отделяне на клиентски средства и активи.	assets in each position in the Register of positions with the Accounting Department periodically and before every operation in accordance with the policy for separation of client funds and assets.
VI. МЕРКИ СРЕЩУ ЗАГУБА НА КРИПТОАКТИВИ, ИЗМАМИ, КИБЕР АТАКИ И НЕБРЕЖНОСТ	**VI. MEASURES AGAINST LOSS OF CRYPTO-ASSETS, FRAUD, CYBER-THREATS AND NEGLIGENCE**
16. **Мерки срещу загуба на криптоактиви, измами, кибер атаки и небрежност** 16.1. Клиентските криптоактиви се съхраняват в специален портфейл/сметка за клиентски криптоактиви в зависимост от вида на криптоактива. 16.2. Само клиентът може да инициира преводи на криптоактиви към и от специалния портфейл/сметка. Процесът е напълно автоматизиран, изключвайки риска от небрежност от страна на представители на Дружеството. 16.3. Дружеството прилага мерки за двуфакторно удостоверяване на всички клиентски поръчки, както е описано в политиката за изпълнение на поръчки и политиката за превод, за да гарантира, че само клиентът има достъп до криптоактивите под попечителство. 16.4. Дружеството прилага мерки за идентифициране на подозрителна активност и изискване на допълнително удостоверяване от клиента, когато е необходимо, за предотвратяване на киберзаплахи. 16.5. Дружеството прилага строги политики за отделяне на клиентските криптоактиви и документиране на клиентските поръчки, за да гарантира, че операциите с клиентски криптоактиви се инициират само от съответния клиент и се изпълняват в съответствие с нареждането на клиента.	**16. Measures against loss of crypto-assets, fraud, cyber-threats and negligence** 16.1. Client crypto-assets are stored in dedicated wallet/account for client crypto-assets depending on the type of crypto-asset. 16.2. Only the client can initiate transfers of crypto-assets to and from the dedicated wallet/account. The process is completely automated, excluding the risk of negligence of representatives of the Company. 16.3. The Company is applying measures for two-factor authentication of all client orders, as described in the policy for execution of orders and the transfer policy, in order to ensure that only the client has access to the crypto-assets under custody. 16.4. The Company is applying measures for identification of suspicious activity and requiring additional authentication from the client where necessary to prevent cyber threats. 16.5. The Company is applying strict policies for segregation of client crypto-assets and documenting client orders to ensure that operations with client crypto-assets are initiated only by the respective client and are executed in line with the client order.

16.6. Дружеството прилага технически и организационни мерки, за да гарантира, че ключовете за специалните портфейли/сметки за клиентски криптоактиви са защитени от загуба поради инциденти и кибератаки 16.7. Дружеството комуникира с клиента само чрез защитени канали, като гарантира, че трети страни не могат да се намесват в комуникацията и по този начин минимизира риска от измама с информация за Дружеството.	16.6. The Company is applying technical and organizational measures to ensure that the keys for the dedicated wallets/accounts for client crypto-assets are protected against loss due to incidents and cyber-attacks. 16.7. The Company communicates with the client only via secure channels, ensuring that third parties cannot interfere in the communication and thus minimizing the risk of fraud with information about the Company.
17. **Структура на съхранение (горещи/студени портфейли)** 17.1. За да гарантира безопасността на клиентските активи, Компанията използва хибриден модел за съхранение, включващ „студени“ и „горещи“ портфейли. 17.2. По-голямата част от клиентските криптоактиви (целен обем от поне 90-95%) се държат в студени портфейли. Тези портфейли са напълно „изолирани“ (постоянно изключени от интернет), което ги предпазва от онлайн кибератаки и неоторизиран отдалечен достъп. 17.3. Малка част от активите се поддържат в горещи портфейли (свързани с интернет, защитени от инфраструктурата на Fireblocks) единствено за да се осигури ликвидност за ежедневни оперативни тегления и преводи. Балансът в горещите портфейли е стриктно минимизиран, за да покрие непосредствените оперативни нужди.	**17. Storage Structure (Hot/Cold Wallets)** 17.1. To ensure the safety of client assets, the Company utilizes a hybrid storage model comprising "Cold" and "Hot" wallets. 17.2. The majority of client crypto-assets (targeting at least 90-95%) are held in Cold Wallets. These wallets are completely "air-gapped" (permanently disconnected from the internet), protecting them from online cyber-attacks and unauthorized remote access. 17.3. A small portion of assets is maintained in Hot Wallets (connected to the internet, secured by Fireblocks infrastructure) solely to ensure liquidity for day-to-day operational withdrawals and transfers. The balance in Hot Wallets is strictly minimized to cover immediate operational needs.
18. Управление на ключове и многократно подписване (MPC) 18.1. Компанията използва усъвършенствани криптографски технологии, като например схеми за многостранно изчисление (MPC) или многократно подписване, за да елиминира „единични точки на грешка“.	**18. Key Management & Multi-Signature (MPC)** 18.1. The Company employs advanced cryptographic technologies, such as Multi-Party Computation (MPC) or Multi-Signature schemes, to eliminate "single points of failure."

18.2. Частните ключове (или ключови фрагменти в MPC) никога не се генерират, съхраняват или използват от едно лице. 18.3. Авторизацията на всяка промяна в политиката за управление в инфраструктурата на Fireblocks изисква съвместно одобрение от множество оторизирани служители (схема M-of-N). 18.4. Ключовете се генерират и съхраняват в хардуерни модули за сигурност (HSM), сертифицирани по стандартите FIPS 140-2 ниво 3 или по-високи.	18.2. Private keys (or key shards in MPC) are never generated, stored, or used by a single individual. 18.3. Authorization of any management policy change in the Fireblocks infrastructure requires the collaborative approval of multiple authorized personnel (M-of-N scheme). 18.4. Keys are generated and stored within Hardware Security Modules (HSMs) certified to FIPS 140-2 Level 3 or higher standards.
19. Включване в бял списък 19.1. За да предотврати кражба чрез неоторизирани тегления, Компанията прилага строга политика за включване в бял списък на адреси. 19.2. Тегленията могат да се извършват само към външни адреси на портфейли, които са били предварително проверени и добавени към одобрения списък (бял списък) от клиента. 19.3. Добавянето на нов адрес към белия списък изисква силно удостоверяване (2FA) и потенциално забавяне във времето (период на охлаждане), за да се предотврати незабавна кражба в случай на поглъщане на акаунта.	**19. Whitelisting** 19.1. To prevent theft through unauthorized withdrawals, the Company implements a strict Whitelisting Address Policy. 19.2. Withdrawals can only be executed to external wallet addresses that have been previously verified and added to the Approved List (Whitelist) by the client. 19.3. Adding a new address to the Whitelist requires strong authentication (2FA) and potentially a time-delay (cooling-off period) to prevent immediate theft in case of account takeover.
20. Физическа и цифрова сигурност 20.1. Компанията внедрява надеждни защитни стени, DDoS защита и системи за откриване на проникване. Цялата вътрешна комуникация относно управлението на активи е криптирана. Достъпът до административните панели следва „принципа на най-малките привилегии“. 20.2. Физическите резервни копия на ключове (seed phrases) или HSM устройства се съхраняват в географски разпределени, пожароустойчиви и	**20. Physical and Digital Security** 20.1. The Company implements robust firewalls, DDoS protection, and intrusion detection systems. All internal communication regarding asset management is encrypted. Access to administrative panels follows the "principle of least privilege." 20.2. Physical backups of keys (seed phrases) or HSM devices are stored in geographically distributed, fireproof, and access-controlled bank vaults or secure facilities.

контролирани банкови трезори или защитени съоръжения. 20.3. Компанията провежда редовни тестове за проникване и сканирания за уязвимости на своята инфраструктура за съхранение, както е предвидено в Регламента за цифрова оперативна устойчивост (DORA). Физическа и цифрова сигурност.	20.3. The Company conducts regular penetration testing and vulnerability scans of its custody infrastructure as mandated by the Digital Operational Resilience Act (DORA).

Версия на документа/Document version:
16.02.2026