CRYPTSAFE CUSTODY SERVICE TERMS OF USE

1.   Introduction

1.1   CHAINUP CRYPTSAFE PTE. LTD. ("ChainUp") provides customers with digital payment token ("DPT") custody services (the "Services") with greater security, ease of use, and scalability. After years of deep cultivation, the company is in a leading position in the industry in terms of technical professionalism and market foresight. ChainUp's system adopts multi-party computation ("MPC") technology to protect DPTs from hacker attacks and private key single point risk, and leverages whitelists and customizable withdrawal approval processes to increase the security level of users' accounts.

In addition, ChainUp provides a full-link activity monitoring system allowing ChainUp to automatically monitor and record all of a customer's the transaction process from start to end, and ensure that all transactions are processed in accordance with the specified procedures. By using our custody services, you agree to be bound by these terms. If you do not agree, please do not use our services.

2.   Eligibility

2.1   By using our Services, you confirm that you are at least 18 years old and have the legal capacity to enter into these terms. You also confirm that your use of our services complies with applicable laws and regulations.

3.   Services Provided

3.1   Under this service, ChainUp will provide MPC wallets to customers, which will divide a single cryptographic key into three private key shards, each key shard holding a private set of data. Users will hold on to one key shard, while ChainUp will hold on to the remaining two key shards.

3.2   The execution of a transaction will require three key shards to sign and send the transaction. Whenever a key is required, the MPC is set in motion to confirm with all parties simultaneously whether they approve of the request. Parties will independently compute their part of the private key share(s) they hold to produce a signature, without revealing the encryption to other parties.

3.3   Users can provide instructions for the DPT stored in their wallet to be transmitted to another DPT wallet, as long as the user is able to authenticate the transaction using its key shard.

3.4   By default, the MPC wallet uses TRON Energy ("Energy") and TRON Bandwidth ("Bandwidth"), together known as "Resources", instead of traditional gas fees when processing transactions. The interaction of smart contracts requires Energy and Bandwidth, while the transfer of TRX currency only requires Bandwidth. If you do not have enough Energy or Bandwidth, TRX may be deducted to cover the cost.

If you prefer not to use the Resources, you have the option to opt out through the wallet settings. Please review your preferences to ensure they align with your intended transaction method.

4.   Account Creation and Maintenance

4.1   To use our services, you must create an account by providing accurate and complete information. You are responsible for maintaining the confidentiality of your account credentials and for all activities that occur under your account. You shall notify us immediately if you notice any unauthorized use of your account.

4.2   Whenever a customer requests any action of ChainUp, it will be required to provide its instructions. ChainUp acts upon instructions given by its customers or any person authorised by its customers to give instructions to it or perform other operations through ChainUp's website on behalf of its customers ("Authorised Persons") that are received and verified by ChainUp pursuant to this Agreement. Any instructions given will continue in full force and effect until cancelled (if possible) or executed.

4.3   The customer is required to maintain an updated and current list of Authorised Persons at all times on ChainUp and will immediately notify ChainUp of any changes to the list of Authorised Persons by updating the list on the platform, including for termination of employment, or otherwise. The customer shall make available all necessary documentation and identification information, as reasonably requested by ChainUp to confirm:

(a)   the identity of each Authorised Person;

(b)   that each Authorised Person is eligible to be deemed an "Authorised Person" as defined above; and

(c)   that the person(s) requesting the changes in the list of Authorised Persons have valid authority to request changes on behalf of the customer.

4.4   ChainUp shall be entitled to rely upon any instructions it receives from an Authorised Person (or from a person reasonably believed by ChainUp to be an Authorised Person) in accordance with this Agreement. ChainUp may assume that any instructions received from a customer or Authorised Person are not in any way inconsistent with the provisions of organisational documents of the customer or of any vote, resolution, or proper authorisation and that the customer is authorised to take the actions specified in the instructions.

4.5   The customer must verify all transaction information prior to submitting instructions to ChainUp. ChainUp shall have no duty to inquire into or investigate the validity, accuracy or content of any instructions. If any instructions are ambiguous, incomplete, or conflicting, ChainUp may refuse to execute such instructions until any ambiguity, incompleteness, or conflict has been resolved. ChainUp may refuse to execute instructions if, in its sole opinion, such instructions are outside the scope of its duties under this Agreement or are contrary to any applicable laws.

ChainUp will provide customers, on a real-time basis, the following particulars in the form of electronic records stored on an electronic facility accessible through ChainUp's website at the following link: https://custody.chainup.com/login under "Transactions":

(a) transactions to purchase or sell assets entered into by the customer and the price at which the transactions are entered into;

(b) the status of every asset (including DPT) in ChainUp's custody held for the customer, including any asset (including DPT) deposited with a safeguarding person (if any);

(c) the movement of every asset (including DPT) of the customer, the date of and reasons for such movement, and the amount of the asset (including DPT) involved;

(d) the movement and balance of relevant money received from, or on account of, the customer in respect of the provision of the Services (if any); and

(e) a detailed account of all financial charges and credits to the customer's account during the monthly statement period, unless the detailed account of financial charges and credits has been included in any contract note or tax invoice issued by ChainUp to the customer.

By using our Services, you consent to the particulars above being made available to you in this manner and the above shall suffice as the provision of a statement of account, and you consent to not receive any separate statement of account from ChainUp on a monthly basis.

5. Security Measures

5.1 ChainUp will retain control over access to the underlying DPT in the MPC wallets it provides in the following ways –

(a) ChainUp will hold two of the three key shards of each MPC wallet;

(b) As all three key shards are required to execute a DPT transaction to or from the MPC wallet, ChainUp would have the ability to co-authorise a transaction by signing the two key shards it holds; and

(c) ChainUp may, in rare circumstances (such as when transaction monitoring checks are failed) block the execution of a transaction, either by way of the KYT transaction monitoring tool or by withholding ChainUp's signing of the two key shards that ChainUp holds.

5.2 The MPC wallets allow for the function for users to provide instructions for the DPT stored in its MPC wallet to be transmitted to another DPT wallet, as long as the user is able to authenticate the transaction using its key shard. Following on from this, ChainUp would be providing DPT Safeguarding Services under the PS Act.

5.3 Additionally, ChainUp would not only be facilitating the transfer of DPT and moving DPT from one account to another (i.e., either from a user's MPC wallet to another DPT wallet, or from another DPT wallet to a user's MPC wallet), it would also be in possession of such DPT being transferred. Following on from this, ChainUp would be providing DPT Acceptance Services and DPT Arrangement Services under the PS Act.

5.4 Where appropriate, ChainUp use available technology to protect the security of communications made through our ChainUp website. Do note that ChainUp do not accept liability for the security, authenticity, integrity or confidentiality of any transactions and other communications made through our ChainUp website. Internet communications may be susceptible to interference or interception by third parties. ChainUp will do our best but ChainUp cannot make any warranties that our ChainUp website is free of infection by computer viruses or any other unauthorised software.

6. Tokens Supported

6.1 ChainUp will support the following tokens on its platform: BTC, ETH, BCH, LTC, ETC, BSV, USDC, USDT, TRX, MATIC, and FIL. It may be the case that further tokens will be supported in the future.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT EMPTY

7. Hosting Fee

One-time Installation Fee (USDT)	Quarterly Withdrawal Amount (USDT)	Quarterly Withdrawal Rates	Quarterly Minimum spend (USDT)
5,000	0-10 million	0.080%	**8000**
	10-50 million	0.059%	
	50-100 million	0.048%	
	100-200 million	0.042%	
	200-500 million	0.028%	
	More than 500 million	Customization	

7.1 Fee Description.

(a) If the quarterly withdrawal amount is $12,000,000: quarterly fee = 12,000,000 * 0.059% = $7,080, less than the minimum purchase of $8,000, you need to pay $8,000

(b) If the quarterly withdrawal amount is $60,000,000: quarterly fee = 60,000,000 * 0.048% = $28,800, which is greater than the minimum purchase of $8,000, you need to pay $28,800

(c) If the withdrawal currency is a non-stablecoin, ChainUp's fees will be calculated according to the exchange rate (based on the rate published on HTX) for USDT and converted into USDT according to the price at the time of withdrawal. This exchange rate will be displayed to the customer at the point of transaction. The type of DPT withdrawn by the customer will remain the same.

7.2 ChainUp reserves the right to revise its fees at any time after the first anniversary of the commencement of this Agreement if it provides the customer with at least 30 days' advance notice of such a revision. ChainUp will exercise this right of review no more than annually, following a comprehensive review of fees and considering all relevant factors.

8. Custody and Control

8.1 While ChainUp holds your digital assets in custody, you retain ownership and control over them. ChainUp will not use, lend, or leverage your assets for any purpose other than those specified in these terms or as instructed by you.

9. Transaction Processing

9.1 You may instruct us to execute transactions involving your digital assets. ChainUp will process these transactions in accordance with your instructions, provided they comply with our security procedures and legal requirements.

10. Liability

10.1 To the maximum extent permitted by applicable law and subject to the exceptions provided in clause 10.3 below, in no event shall ChainUp, its affiliates and service providers, or any of their

respective officers, directors, agents, employers or representatives, be liable for any lost profits or any special incidental, indirect, intangible, or consequential damages, whether based in contract, tort, negligence, strict liability, or otherwise, arising out of or in connection with authorised or unauthorised use of the Services, or this Agreement, even if ChainUp has been advised of or knew or should have known the possibility of such damages.

10.2 To the maximum extent permitted by applicable law and subject to the exceptions provided in clause 10.3 below, in no event shall the aggregate liability of ChainUp, its affiliates and service providers, or any of their respective officers, directors, agents, employees or representatives, exceed the fees paid or payable to ChainUp under this Agreement during the 3-month period immediately preceding the first incident giving rise to such liability.

10.3 The exclusions and limitations of liability in clause 10.1 and clause 10.2 will not apply to ChainUp's fraud, wilful misconduct, or gross negligence. ChainUp's liability for gross negligence shall be limited to the value of the affected digital assets or fiat currency.

10.4 In the event of losses of customers' digital assets arising from fraud or negligence on the part of ChainUp, ChainUp will act in accordance with its compensation framework. Under this framework:

(a) Customers are advised to promptly report any losses and associated suspicious activity to ChainUp's support team through custody@chainup.com

(b) ChainUp will investigate the matters and endeavour to provide a resolution within 30 days. In any event, ChainUp will provide the affected customer with an updated within this timeline;

(c) As part of ChainUp's investigations into the matter, ChainUp may contact the customer and/or any other relevant third parties for further information; and

(d) If the result of ChainUp's investigations reveal that the claim is valid, ChainUp will compensate the customer for any direct losses suffered by the customer in connection with ChainUp's fraud or negligence. Notwithstanding this, if a customer may potentially be able to make a claim under any form of insurance coverage, the customer shall not be entitled to such compensation by ChainUp to the extent of the sum insured.

11. User Obligations

11.1 You agree to:

(d) comply with all applicable laws and regulations;

(e) provide accurate and complete information;

(f) keep your account credentials secure; and

(g) promptly update us on any changes to your information.

12. Termination

12.1 ChainUp may terminate or suspend your account at our discretion if you violate these terms or if required by law. You may terminate your account by providing us with written notice. Upon termination, ChainUp will return your digital assets to you, subject to any outstanding obligations.

13.   Amendments

13.1   ChainUp may amend these terms from time to time. ChainUp will notify you of any material changes. Continued use of our services after such changes will constitute your acceptance of the amended terms.

14.   Governing Law

14.1   These terms are governed by the laws of Singapore. Any dispute arising out of or in connection with this contract, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre ("SIAC") in accordance with the Arbitration Rules of the Singapore International Arbitration Centre ("SIAC Rules") for the time being in force, which rules are deemed to be incorporated by reference in this clause. The seat of the arbitration shall be Singapore. The Tribunal shall consist of 1 arbitrator appointed by ChainUp. The language of the arbitration shall be English.

15.   Contact Information

15.1   ChainUp will use commercially reasonable efforts: (i) to provide reasonable technical support to customers, by email or telephone, during ChainUp's normal business hours from 10am-7pm (UTC + 8); (ii) to respond to support requests in a timely manner; and (iii) resolve such issues by providing updates and/or workarounds to customers (to the extent reasonably possible and practical), consistent with the severity of the issues identified in such requests and their impact on the customer's business operations.

15.2   If you have any questions or concerns about these Terms of Use, please contact us via our official website at https://www.chainup.com/.

16.   Consumer Protection Disclosures

16.1   ChainUp is a Singapore-incorporated private limited company which has been granted an exemption from holding a licence under the Payment Services Act 2019 pursuant to the Payment Services (Amendment) Act 2021 (Saving and Transitional Provisions) Regulations 2024 to provide DPT services. If you are a customer in Singapore, ChainUp may provide you with the Services. The other regulated services described on ChainUp's website will not be available to you if you are a customer in Singapore.

16.2   The key risks of the Services are set out below:

Digital asset custody involves various forms of assets such as cryptocurrency, digital securities, non-fungible tokens (NFTs), etc. Although custody services aim to enhance asset security and compliance, there are still a series of specific risks in this field. Thorough threat and risk assessment is key to ensuring asset security, complying with laws and regulations, and resisting potential threats. The following are the main types of risks that need to be considered in digital asset custody.

Technical risk
- Hacking attacks: Even the most advanced security systems can be subject to hacking attacks, including intrusions into trading systems, physical attacks on cold storage facilities, etc.
- System failure: Software defects, hardware failures, or data centre issues can cause service interruptions and affect the availability of assets.

- Loss or leakage of private key: Secure management of private key is the core of digital asset security. Loss or leakage of private key will make related assets irretrievably lost.

Operational risk
- Internal Threats to Employees: Risk of employees abusing their access for illegal transactions or theft of assets.
- Risks of third-party service providers: Relying on third-party services (such as Cloud as a Service provider) may increase operational risks, and problems with these services may indirectly affect the security and stability of managed services.

Market risk
- Asset Volatility: The prices of cryptocurrencies and other digital assets are extremely volatile. Market crashes or sharp fluctuations can cause asset values to rapidly decline.
- Liquidity Risk: Under certain market conditions, some digital assets may be difficult to liquidate immediately.

Nonetheless, ChainUp has a Risk Mitigation Strategy to mitigate the above risks. ChainUp recognises that it is crucial to adopt effective risk mitigation strategies to address these risks to consumers.

Technical risk
- Multi-factor authentication: A multi-factor authentication (MFA) policy is in place to enhance account security.
- Distributed Denial of Service (DDoS) Protection: By adopting advanced DDoS mitigation tools and strategies, ChainUp's systems and policies are better able to protect hosted platforms from attacks.
- Cold storage: ChainUp keeps 90% of customers' assets in cold wallets that are not connected to the internet to reduce the risk of hacking.
- Regular security audits: Regular security audits and penetration testing exercises are conducted to identify and fix potential security bugs and other system vulnerabilities.

Operational risk
- Disaster Recovery Plan: ChainUp regularly updates its Disaster Recovery and Business Continuity Plan to ensure that managed services can quickly recover in the event of an emergency.
- Technical maintenance: Regular maintenance and upgrades of the system are in place to reduce the risk of technical failure.
- Employee training: Safety awareness and compliance training for employees are in place to reduce the risk caused by operational errors. In managing employee access to customer information, ChainUp applies the principles of "never alone", "segregation of duties", and "least privilege" so that no one person has access to perform sensitive system functions.

Market risk
- Diversification: ChainUp advises its clients to diversify their investments to reduce the impact of market volatility.
- Market monitoring: ChainUp closely monitors market trends and responds promptly to significant events that may affect client assets.
- Price Warning System: ChainUp provides a price warning system to help clients monitor and manage market fluctuations.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT EMPTY

17. **Risk Warning**

Before you:

(a)   Pay your DPT service provider any money or DPT; or

(b)   pay a third party any money or DPT under an arrangement by your DPT service provider,

you should be aware of the following.

1.   Your DPT service provider has been granted an exemption from holding a licence under the Payment Services Act 2019 pursuant to the Payment Services (Amendment) Act 2021 (Saving and Transitional Provisions) Regulations 2024 to provide DPT services. Please note that this does not mean you will be able to recover all the money or DPTs you paid to your DPT service provider or any other third party referred to above, if your DPT service provider's or the third party's business fails.

2.   You should be aware that MAS does not supervise or regulate your DPT service provider for the provision of unregulated services.[1] This includes any service of trading digital payment token derivatives such as futures.

3.   You should not transact in the DPT if you are not familiar with this DPT. This includes how the DPT is created, and how the DPT you intend to transact is transferred or held by your DPT service provider.

4.   You should be aware that the value of DPTs may fluctuate greatly. You should buy DPTs only if you are prepared to accept the risk of losing all of the money you put into such tokens.

5.   You should be aware that ChainUp, as part of its exemption from holding a licence to provide DPT services, may offer services related to DPTs which are promoted as having a stable value, commonly known as "stablecoin".

18. **Safeguarding of Digital Assets**

18.1   Each customer's assets are independently held, which means that the assets of each customer will not be mixed together. They are all located at the customer's own address and are kept independently by the customer

18.2   Customers will receive timely notifications through our platform regarding any entitlements accruing to their digital assets. Any such entitlements will be deposited into the customer's custodial accounts held with ChainUp. To view and access their entitlements, customers can login to ChainUp's platform and navigate to https://custody.chainup.com/login

18.3   ChainUp's storage system uses MPC technology, multi-signature technology, and multi-authentication, combined with hardware isolation for asset project management, to protect digital assets from hacker attacks and theft. At the same time, it uses allowlist and customizable withdrawal approval process to improve account security level.

---

[1] Please refer to Section 2.3.1 of the Guide to the Payment Services Act 2019 (which can be found on the MAS website) for the types of payment services which are regulated under the Payment Services Act 2019. Services which do not fall within the list of services in Section 2.3.1 are unregulated services.

Distributed key storage technology

ChainUp uses distributed key storage technology, allowing users to generate and manage all private key sharding. Among them, users save one private key locally, while the other two are stored on Amazon Cloud and Microsoft Cloud respectively in Singapore. This distributed storage method combines hardware isolation technology, allowing users to fully control their assets. ChainUp supports 3-3 TSS configuration; when users initiate transaction signatures, these three private key sharding will participate in the signature at the same time, eliminating the single point of failure problem in private key management and significantly improving the security of asset self-management, ensuring that users' investment assets reach the highest level of security in the market.

Full-process node monitoring and auditing

Users can customize trading strategies. Asset trading orders subject to risk control need to be approved by designated co-management members. Only after reaching a specific approval threshold can they enter the final signature broadcast stage. At the same time, full-process node monitoring is provided, allowing users to intuitively understand the status of trading orders at each stage, ensuring clear and complete approval flow, not only meeting internal control and financial audit needs, but also ensuring the security and credibility of transactions.

18.4 ChainUp will at all times store at least 90% of its customers' digital assets in cold wallets and not more than 10% in hot wallets. Customers will be entitled to allocate a greater percentage of their assets to stored in cold wallets, provided that the percentage of each customer's assets stored in cold wallets does not fall below 90%.

19. Conflicts of Interest

19.1 As a provider of a broad range of financial services, ChainUp may face actual and potential conflicts during the course of its activities. These may arise from any one or combination of the following:

(a) ChainUp and its customer relationships;

(b) ChainUp and any other third-party service provider duties;

(c) Employee interests which potentially compete with ChainUp products or services; and

(d) Potentially competing interests between two or more customers.

19.2 ChainUp utilises various means to prevent and manage conflicts of interest, which include the following:

(a) Employee compliance policies and directives that require disclosure, monitoring and reporting of conflicts of interest that arise involving an employee, ChainUp, and/or a customer;

(b) Clear governance rules relating to the handling and management of third-party relationships;

(c) Mandatory legal, risk and compliance reviews monitoring whether specific activities will give rise to conflicts of interest; and

(d) Provision of internal guidance and training on the handling and disclosure of conflicts of interest.

19.3 ChainUp discloses conflicts of interest in cases where it is not possible to avoid or resolve the conflict. Such disclosure is made in a clear and direct manner, using the appropriate medium.

20. Customer Account Setup

20.1 The customer agrees to provide ChainUp with the information ChainUp requests (which ChainUp may request at any time deemed necessary) for the purposes of identity verification and the detection of money laundering, terrorist financing, fraud, or any other financial crime, and permit ChainUp to keep a record of such information. The customer will need to complete certain verification procedures before the customer is permitted to start using the Services.

20.2 The information ChainUp requests may include but is not limited to personal information such as the customer's full name (including any aliases), unique identification number, residential/registered/business address, telephone number, email address, date of birth or incorporation/establishment/registration, nationality, and any such information that ChainUp is required to collect from time to time under applicable law.

20.3 The customer may also be required to undergo enhanced due diligence procedures, where ChainUp may request that the customer submit additional information about itself and its business, provide relevant records, and arrange for meetings with ChainUp's staff so that ChainUp may, among other things, establish the source of the customer's wealth and source of funds for any transactions carried out in the course of the customer's use of the Services.

20.4 In providing ChainUp with this or any other information that may be required, the customer confirms that the information is true, accurate and complete, and the customer has not withheld any information that may influence ChainUp's evaluation of the customer for the purposes of the customer's use of the Services. The customer undertakes to promptly notify in writing and provide ChainUp with information regarding any changes in circumstances that may cause any such information provided to become false, inaccurate or incomplete and also undertake to provide any other additional documents, records and information as may be required by ChainUp and/or applicable law. The customer permits ChainUp to keep records of such information. ChainUp will treat this information in accordance with applicable data protection laws.

20.5 ChainUp reserves the right, at its sole discretion, to create, manage, suspend, freeze and terminate user accounts, including in (but not limited to) circumstances where MAS (or any other Government authority or regulator) has made any suggestion, direction or instruction to take such action in respect of user accounts or where the account has breached ChainUp internal governance policies

20.6 By registering for and using our Services, you agree that ChainUp may take any necessary actions related to account creation, including but not limited to verification, approval, suspension, freezing or deletion of accounts. ChainUp also reserves the right to request additional information from you to facilitate the account creation process. Failure to comply with such requests may result in the denial or termination of your account.

By using our custody services, you acknowledge that you have read, understood, and agree to these Terms of Use.