Yeap Protocol Risk Disclosures

Version dated 10 September 2025

I. Introduction

Purpose: This Risk Disclosure document is designed to inform users of the Services, services and related information and materials offered by the Yeap Labs and the Interface and related services that facilitate interaction with the Yeap Protocol, of the potential risks associated with using the Yeap Protocol. In addition to the terms defined elsewhere herein, capitalized terms will have the meanings defined in the terms of service posted on the Site.

These disclosures aim to provide clarity on the inherent uncertainties and responsibilities involved in interacting with decentralised finance (DeFi) platforms.

Scope: The disclosures outlined herein apply to all interactions with the Yeap Protocol, including the use of its smart contracts, participation in its governance, and engagement with its associated services, including services deployed, designed, permitted access to, utilised, modified, or deployed by any third party.

General: The Yeap Protocol is a DeFi application designed to provide technology services. By engaging with the Yeap Protocol, you acknowledge and accept that you are participating in a highly experimental and rapidly evolving space.

The risks associated with protocols and applications like the Yeap Protocol are significant, and you should only use the Yeap Protocol if you fully understand these risks and can bear full losses.

Under no circumstances will we be liable for any loss or damage resulting from your use of the Yeap Protocol.

II. Experimental Nature

The Yeap Protocol and all related software, including blockchain technology, smart contracts, vaults, and digital asset wallets are experimental and in continuous development. The Yeap Protocol is provided "As Is" "Where Is" and "As Available" without any warranties, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, or non-infringement. Users should be aware that the experimental nature of the Yeap Protocol could lead to unexpected outcomes, including the total loss of assets that interact with the Yeap Protocol.

III. General Risks

Volatility of Cryptocurrency Markets: The cryptocurrency markets are highly volatile, with prices fluctuating widely in short periods. This volatility can significantly affect the value of assets held within the Yeap Protocol, and a given person's ability to access services, products, transactions, or assets facilitated by the operation of the Yeap Protocol.

Regulatory Risks and Legal Uncertainty: The legal landscape for DeFi is evolving. Changes in regulations, positions of regulators, legislative enactments, or enforcement actions could impact your ability to use the Yeap Protocol or result in adverse legal consequences. Users should stay informed about the legal environment that may affect their use of digital assets, cryptocurrencies, digital assets wallets, DeFi, smart contracts and the Yeap Protocol and should comply with all applicable laws.

IV. Security Risks

Cyberattacks and Hacking: The Yeap Protocol, like all DeFi platforms, is susceptible to cyberattacks, hacking, and other security breaches. While we implement rigorous security measures, no system is entirely immune to threats. Risks include, but are not limited to, phishing, malware, distributed denial-of-service (DDoS) attacks, "zero days," and other malicious activities.

Smart Contract Vulnerabilities: Despite rigorous testing and auditing, smart contracts may still contain vulnerabilities, such as re-entrancy attacks, front-running, timestamp manipulation, inherited vulnerabilities from third party libraries, and other potential exploits. Users should be aware that exploiting these vulnerabilities could lead to a loss of access to, control of, or use of assets, and significant financial losses.

Nation-State and Black Hat Attacks: The Yeap Protocol, like other blockchain systems, may be targeted by highly sophisticated cyberattacks from nation-state actors or "black hat" i.e. malicious hackers. These attackers may exploit known or unknown vulnerabilities, resulting in severe disruptions or loss of assets.

Unknown Vulnerabilities: As technology evolves, new vulnerabilities may be discovered that could affect the security of the Yeap Protocol. These include potential risks from advances in cryptography, such as quantum computing, which could undermine current blockchain security measures. Although we have undertaken reasonable, market standard practices to identify vulnerabilities in the Yeap Protocol, we do not guarantee that the Yeap Protocol is free of any defect, flaw or vulnerability.

Risk of Theft: There is no assurance against the theft of digital assets due to sophisticated cyber-attacks or exploitation of vulnerabilities in the Yeap Protocol, the underlying infrastructure relied upon by the Yeap Protocol or users of the Yeap Protocol including digital assets wallets, blockchain(s), or associated third-party services, service providers, or functions not within our control. Such incidents could lead to the partial or complete loss of access to, control of or use of your assets.

Service Availability: The Yeap Protocol may experience downtime or become inaccessible due to maintenance, third-party service disruptions, attacks or compromises of third-party services or products, or blockchain network congestion, attacks or related issues. We do not guarantee continuous availability or functionality of the Yeap Protocol, and users should be prepared for potential interruptions to access, or to functionalities provided by the Yeap Protocol.

V. Technical Risks

Software Bugs and Technical Failures: The Yeap Protocol operates on complex software that may contain bugs or experience failures, potentially leading to loss of assets, access to assets, or interruption of services. These risks may be increased by the rapid pace of technological change, which may introduce new unforeseen vulnerabilities or attack vectors that may impact the function, availability, and security of the Protocol.

Impact of Advances in Technology: Emerging technologies, such as quantum computing, may pose future risks to the security of blockchain-based systems and systems built upon and that rely on encryption of underlying systems, including the Yeap Protocol. Users should be aware that such advances could undermine the cryptographic security relied upon by the Yeap Protocol.

Flawed Logic and Design: The underlying logic and design of the Yeap Protocol and related software may be flawed, defective, or impaired. This could result in the Protocol operating incorrectly or not as intended, leading to unintended transactions or losses of a loss of access to, control of, or use of assets, and significant financial losses.

VI. Protocol-Specific Risks

Smart Contract Risks: The Yeap Protocol's smart contracts are designed to be secure but are not infallible. Vulnerabilities may exist, and their exploitation could lead to a loss of access to, control of, or use of assets, and significant financial losses.

Liquidation Risks: Similar to other collateralized systems, the Yeap Protocol is designed with user asset liquidation as part of its core functionalities. Such properties are likely to also exist in other products and services created by users of the Services. Users are expected to monitor the health of their positions, including accounts for collateral and borrowed assets, and their values. Failure to do so may result in liquidation by third parties which may be initiated programmatically or by third parties which may include the Company. Such liquidations are irreversible.

Functionality and Performance: we do not guarantee continuous, uninterrupted, error-free, timely or expected operation of the Yeap Protocol. Users should be aware of potential issues that may impact its functionality and performance.

User Interface: Certain user interface elements or design decisions within the Yeap Protocol may be complex, confusing or unclear to some users, which may result in a User executing a different action or transaction than that user may have intended or desired. Users are advised to proceed with caution and verify their actions before finalising any transactions. Users may access documentation explaining the functions of the Yeap Protocol at docs.yeap.finance.

Governance Risks: Certain aspects of the Yeap Protocol may be governed by a decentralised community. Proposals made and accepted through documented governance processes could alter the protocol in ways that may affect users of the Yeap Protocol, its features, products, services, functionalities, and the transactions which may or may not be conducted using various aspects of the Yeap Protocol. These changes are outside our control, and we expressly disclaim any and all liability for any negative impacts resulting from governance decisions.

VII. Third-Party Risks

Reliance on Third-Party Services and Data: The Yeap Protocol may rely on third-party services, including smart contracts, oracles, and data feeds. Failures, flaws, delays, compromises, attacks on, manipulations of, and defects or inaccuracies in these third-party services could negatively impact the Yeap Protocol's operation or lead to incorrect or unexpected transaction executions and transaction execution outputs, and could lead to a loss of access to, control of, or use of assets, and significant financial losses.

Third Party- related Risks: Certain functions within the Yeap Protocol or its underlying blockchain may depend on timely actions by third parties. Delays or failures of those Third Parties could result in inaccessibility of protocol functionality or loss of assets.

VIII. Open-Source and Experimental Technology

The Yeap Protocol relies on open-source and experimental technology, and there are inherent risks associated with using DeFi services, products, applications and protocols built on this technology. These risks include, but are not limited to, smart contract vulnerabilities, potential loss of digital assets, and unforeseen interactions with other blockchain protocols or events, lack of warranties or other performance guarantees, lack of maintenance obligations, cyberattack vulnerabilities, and potential intellectual property infringement claims.

IX. User Responsibility

Legal Compliance: Users are solely responsible to ensure that their use of the Yeap Protocol complies with all applicable civil, criminal, and regulatory laws, regulations and duties, as may apply, including tax obligations, anti-money laundering (AML) regulations, and other relevant legal requirements applicable in their jurisdiction. Users must not use the Yeap Protocol in a manner that

violates any duties, laws or regulations, including those related to AML, counter-terrorist financing, and trade sanctions. Users should not use the Yeap Protocol to avoid or circumvent compliance with any civil, criminal or regulatory law, duty, or obligation.

Self-Custody: Users are fully responsible for the security of their private keys and other credentials required to interact with their own assets and with the Yeap Protocol, and any product, system or application using any part of the Yeap Protocol. Any loss of access to private keys or other access credentials due to negligence or malicious activity is solely the user's responsibility, and we cannot recover lost keys or reverse transactions.

Transaction Accountability: All transactions performed using the Yeap Protocol are final, irrevocable, and irreversible. Users must understand the implications of their transactions and should conduct thorough due diligence before interacting with the Yeap Protocol.

Securing Digital Assets: Users are responsible for securing their digital assets, including the use of secure digital asset wallets and should conduct appropriate information security practices to protect against unauthorised access. Loss or compromise of private keys or other access credentials can result in irreversible and complete loss of access to, control of or use of assets.

Due Diligence and Professional Advice: Users should conduct thorough research and consider seeking professional financial, legal, tax, and technological advice before engaging with the Yeap Protocol.

X. Legal Uncertainty

Impact of Legal Changes: The DeFi space is subject to potential legal changes that could affect the legality and functionality of the Yeap Protocol. Users should be prepared for such changes and ensure compliance with all relevant civil, criminal and regulatory legal obligations related to the ownership and control of digital assets, and the use of the Yeap Protocol.

Legal Risks and Compliance: Our activities are subject to various laws and regulations in the countries where we operate. Regulatory actions, orders, or inquiries may adversely affect the Yeap Protocol and its availability. Additionally, changes in applicable laws or evolving interpretations of existing laws could increase compliance costs, impact the Yeap Protocol's functionality, or necessitate the acquisition of specific licences.

XI. No Professional Advice or Fiduciary Duties

Information Disclaimer: All information provided by us and our affiliates, whether on our Site, platforms, or communications, is intended for informational purposes only. It does not constitute financial, legal, or professional advice, and should not be relied upon as such. Users are encouraged

to seek independent professional advice tailored to their specific circumstances before making any financial decisions related to the use of the Yeap Protocol.

No Fiduciary Relationship: we do not act as an advisor or fiduciary to any user. Neither the we nor the Yeap Protocol nor its governors owe any fiduciary duties to users, and by using the Yeap Protocol, users agree that they alone are responsible for their financial decisions and actions.

XII. Assumption of Risks and Limitation of Liability

User Assumption of Risk: By using the Yeap Protocol, users acknowledge and accept all associated risks, including those related to the security, functionality, and regulatory environment of the Yeap Protocol. Users acknowledge that participating in DeFi involves significant risks, and they should only engage with the Yeap Protocol if they are fully aware of and willing to accept these risks.

Limitation of Liability: To the fullest extent permitted by law, we and our representatives are not liable for any losses, damages, or claims arising from the use of the Yeap Protocol. This includes, but is not limited to, losses resulting from security breaches, regulatory actions, service interruptions, or any other risks described in this risk disclosure. Users agree to hold us harmless from any claims or liabilities related to their use of the Yeap Protocol.

XIII. Incident Reporting and Transparency

Incident Disclosures: we are committed to transparency. Any significant incidents, such as security breaches, manipulation attempts, or major protocol failures, will be disclosed to the community promptly. However, we cannot guarantee the prevention of such incidents and disclaims all liability for any losses arising from them.

XIV. Mitigation Strategies

Audits and Security Measures: The Yeap Protocol has undergone extensive security audits by third-party firms. Additionally, we may operate a bug bounty program to encourage the identification and reporting of vulnerabilities. While these measures are in place to enhance security, they do not eliminate all risks, and it's imperative that users remain vigilant.

XV. Acknowledgment of Risks

By using the Yeap Protocol, you acknowledge that you have read, understood, and agree to this risk disclosure policy. You accept all risks associated with using the protocol and agree that we are not liable for any losses or damages, whether direct or indirect, arising from your use of the protocol.