Responsible Risk Disclosure Policy

This document provides you with information about the risks associated with investment products in which you may invest through the services provided to you by Platanaso.

Platanaso is a community-driven token created on the Binance Smart Chain. All holders will be rewarded in stablecoins. Platanaso will donate toward humanitarian efforts and causes in the tropical communities, while bringing crypto education to various communities, physically and virtually. Your use of the Platanaso platform involves various risks, including, but not limited to, losses while digital assets are being supplied to the platform and losses due to the fluctuation of prices of tokens in a trading pair. Before using the Platanaso, you should review the relevant documentation to make sure you understand how the Platanaso works. You are responsible for doing your own diligence on those interfaces to understand the fees and risks they present.

Cryptocurrency is a digital representation of value that functions as a medium of exchange, a unit of account, or a store of value, but it does not have legal tender status. Cryptocurrencies are sometimes exchanged for FIAT currencies around the world, but they are not generally backed or supported by any government or central bank. Their value is completely derived from market forces of supply and demand, and they are more volatile than traditional currencies. The value of cryptocurrency may be derived from the continued willingness of market participants to exchange fiat currency for cryptocurrency, which may result in the potential for a permanent and total loss of value of a particular cryptocurrency should the market for that cryptocurrency disappear.

Regulatory Landscape

Cryptocurrencies currently face an uncertain regulatory landscape in many jurisdictions. In addition, many cryptocurrency derivatives are regulated by the provisions of national and supra-national (i.e., EU) securities legislation; moreover, some state securities regulators have

cautioned that many initial coin offerings are likely to fall within the definition of a security and subject to their respective securities laws. One or more jurisdictions may, in the future, adopt laws, regulations, or directives that affect cryptocurrency networks and their users. Such laws, regulations, or directives may impact the price of cryptocurrencies and their acceptance by users, merchants, and service providers.

Legislative and regulatory changes or actions at the state, federal, or international level may adversely affect the use, transfer, exchange, and value of cryptocurrency.

Purchasing cryptocurrencies comes with a number of risks, including volatile market price swings or flash crashes, market manipulation, and cybersecurity risks. In addition, cryptocurrency markets and exchanges are not regulated with the same controls or customer protections available in equity, option, futures, or foreign exchange investing. There is no assurance that a person who accepts a cryptocurrency as payment today will continue to do so in the future.

Investors should conduct extensive research into the legitimacy of each individual cryptocurrency, including its platform, before investing. The features, functions, characteristics, operation, use, and other properties of the specific cryptocurrency may be complex, technical, or difficult to understand or evaluate. The cryptocurrency may be vulnerable to attacks on the security, integrity, or operation, including Attacks using computing power sufficient to overwhelm the normal operation of the cryptocurrency's blockchain or other underlying technology. Some cryptocurrency transactions will be deemed to be made when recorded on a public ledger, which is not necessarily the date or time that a transaction may have been initiated.

Cryptocurrency trading requires knowledge of cryptocurrency markets. In attempting to profit through cryptocurrency trading you must compete with traders worldwide. You should have appropriate knowledge and experience before engaging in substantial cryptocurrency trading.

Any individual cryptocurrency may change or otherwise cease to operate as expected due to changes made to its underlying technology, changes made using its underlying technology, or changes resulting from an attack. These changes may include, without limitation, a "fork," a "rollback," an "airdrop," or a "bootstrap." Such changes may dilute the value of an existing cryptocurrency position and/or distribute the value of an existing cryptocurrency position to another cryptocurrency.

Blockchain Risks

Since blockchain is an independent public peer-to-peer network and is not controlled in any way or manner by Platanaso, we shall not be responsible for any failure and/or mistake and/or error and/or breach which shall occur in the blockchain ecosystem or in any other networks in which

the PLATANASO Token may be used and/or traded. You will be bound and subject to any change and/or amendments in the blockchain system and subject to any applicable law which may apply to the blockchain. We make no representation or warranty of any kind, express or implied, statutory or otherwise, regarding the blockchain functionality nor for any breach of security in the blockchain.

Technology

The relatively new and rapidly evolving technology underlying cryptocurrencies introduces unique risks. For example, a unique private key is required to access, use or transfer a cryptocurrency on a blockchain or distributed ledger. The loss, theft, or destruction of a private key may result in an irreversible loss of cryptocurrency associated with this private key. The ability to participate in forks could also have implications for investors. For example, a market participant holding a cryptocurrency position through a cryptocurrency exchange may be adversely impacted if the exchange does not allow its customers to participate in a fork that creates a new product.

The security of the Platanaso ecosystem, and its associated core components, is a top priority for Platanaso. Our Proof of Stake network is secured by the already proven blockchain ecosystem technology and provides valuable services for business or private use. Our mission is to become a layer of trust for digital financial systems at an internet-scale, and the highest level of security is a mandatory prerequisite.

The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet, and Platanaso recognizes that fostering a close relationship with the community will help improve the security of the Platanaso ecosystem. So, if you have information about a vulnerability in the Platanaso ecosystem and associated components, we want to hear from you.

Cybersecurity

The cybersecurity risks of cryptocurrencies and related “wallets” or spot exchanges include hacking vulnerabilities and a risk that publicly distributed ledgers may not be immutable. A cybersecurity event could result in a substantial, immediate, and irreversible loss for market participants that trade cryptocurrencies. Even a minor cybersecurity event in a cryptocurrency is likely to result in downward price pressure on that product and potentially other cryptocurrencies.

Access risks

There are a series of inherent risks with the use of the mobile and/or web-based trading technology such as latency in the prices provided, and other issues that are a result of connectivity (including, without limitation, the use of mobile networks). Prices displayed on the Trading Platform are solely an indication of the executable rates and may not reflect the actual executed or executable price of an order.

The Platform may utilize public communication network circuits for the transmission of messages. Platanaso shall not be liable for any and all circumstances in which you experience a delay in price quotation or an inability to trade caused by network transmission problems or restrictions or any other problems outside our direct control, which include but are not limited to the strength of the mobile signal, network latency, or any other issues that may arise between you and any internet service provider, phone service provider or any other service provider. Please note further that some of the features available on the Trading Platform may not be available on any mobile application.

Future Platanaso applications may require Users to download and install updates to the application or to their device's operating system as such updates are made available. Failure to do so might lead to certain parts of the Services (including trading functions) becoming inaccessible to Members until such update has been successfully downloaded and installed. Performance issues and security risks may arise if Platanaso mobile applications are used on devices with customized or otherwise non-standard operating software or as a result of other software installed on such devices.

Reporting a Security Issue

In case of any security issue is identified, you are required to send us an email to: **marketing@platanaso.com**

What to include:

- Well-written reports in English will have a higher chance of being accepted
- Reports that include proof of concept code will be more likely to be accepted
- Reports that include only crash dumps or another automated tool output will most likely not be accepted
- Reports that include products & services that are out of scope (see the Scope section below) will not be considered
- Include how you found the bug, the impact, and any potential remediation
- Any plans for public disclosure

What you can expect from us:

- A timely response to your email (within 2 business days).
- An open dialog to discuss issues.
- Credit after the vulnerability has been validated and fixed.

Coordinated Responsible Disclosure Policy

We ask security researchers to keep vulnerabilities and communications around vulnerability submissions private and confidential until a patch is developed to protect the Platanaso Token and its users.

Please do:

- Allow the Platanaso team a reasonable amount of time address security vulnerabilities
- Avoid exploiting any vulnerabilities that you discover
- Demonstrate good faith by not disrupting or degrading Platanaso services, products & data

Platanaso pledges not to initiate legal action against researchers as long as they adhere to this policy.

Responsible Disclosure Process

1. Once a security report is received, the Platanaso team verifies the issue and establishes the potential threat
2. Patches to address the issues will be prepared and tested
3. We update the token technology right away

Out of scope

- Scam & phishing attempts involving Platanaso services
- Lost or compromised secret phrases, Keystore files, or private keys
- Physical vulnerabilities
- Social Engineering attacks
- Functional, UI, and UX bugs such as spelling mistakes
- Descriptive error messages
- HTTP error codes/pages

Project risk

AS DESCRIBED IN THE PLATANASO LICENSES, THE PLATANASO PLATFORM AND SERVICES ARE PROVIDED "AS IS", AT YOUR OWN RISK, AND WITHOUT WARRANTIES OF ANY KIND. Although Platanaso developed much of the initial code for the Platanaso, it does not provide, own, or control the Platanaso, which is run by smart contracts

deployed on the Binance Smart Chain. Upgrades and modifications to the protocol are managed in a community-driven way by holders of the PLATANASO token. No developer or entity involved in creating the Platanaso will be liable for any claims or damages whatsoever associated with your use, inability to use, or your interaction with other users of, the Platanaso, including any direct, indirect, incidental, special, exemplary, punitive or consequential damages, or loss of profits, cryptocurrencies, tokens, or anything else of value.

Contact Us

Get in touch with us at **marketing@platanaso.com**

Whether you want to submit an issue, a recommendation, or have security-related topics to bring up, we're happy to hear from you.

In order to protect the Platanaso ecosystem, we request that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed partners if needed.