Ecoterra

Responsible Risk Disclosure Policy

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

Ecoterra is a blockchain-based product/ecosystem that addresses a range of limitations in the real world caused by the centralization problem. In short, we are providing decentralization services to the ecological industry in the real world, including decentralization of transactional services. The platform provides access to a decentralized protocol on the Ethereum Network that aims to create a system which will completely redefine how society chooses to finance environmental conservation efforts. We are mobilizing the power of the blockchain as a way to tackle climate change, with a percentage of our token transaction fee being directed to environmental organizations while another percentage distributed as reward. The platform provides access to a decentralized protocol that creates an ecosystem where the participants benefit in different ways, govern the future of Ecoterra, and interact with the platform and transact using smart contracts ("Smart Contracts"). Your use of the Ecoterra 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 whenever used in a trading pair. Before using the Ecoterra, you should review the relevant documentation to make sure you understand how the Ecoterra 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 by 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 permanent and total loss of value of a particular cryptocurrency should the market for that cryptocurrency disappear.

Regulatory Landscape

Cryptocurrencies currently still face uncertain regulatory landscapes in many jurisdictions, even though The European Union has just passed the MiCA – Markets in Crypto-Assets regulation. In addition, many cryptocurrency derivatives are regulated by the provisions of national 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. More and more jurisdictions will, 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 Ecoterra, and 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 Ecoterra 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 Ecoterra ecosystem, and associated core components, is a top priority for Ecoterra. Our Proof of Stake network is secured by the blockchain technology and provides valuable services for business or private use. Our mission is to become a layer of trust for transactions at 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 Ecoterra recognizes that fostering a close relationship with the community will help improve the security of the Ecoterra ecosystem. So, if you have information about a vulnerability in the Ecoterra 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. Ecoterra 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 Ecoterra 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 Ecoterra 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.

Project risk

AS DESCRIBED IN THE ECOTERRA DOCUMENTATION, THE ECOTERRA PLATFORM AND SERVICES ARE PROVIDED "AS IS", AT YOUR OWN RISK, AND WITHOUT WARRANTIES OF ANY KIND. Although Ecoterra developed much of the initial code for the Ecoterra, it does not provide, own, or control the Ecoterra, which is run by smart contracts deployed on the Blockchain. Upgrades and modifications to the protocol are managed in a community-driven way by holders of the Ecoterra token. No developer or entity involved in creating the Ecoterra will be liable for any claims or damages whatsoever associated with your use, inability to use, or your interaction with other users of, the Ecoterra, including any direct, indirect, incidental, special, exemplary, punitive or consequential damages, or loss of profits, cryptocurrencies, tokens, or anything else of value.

Risk of Losing Access. Loss of Private Key(s), Custodial Error or Personal Error

A private key, or a combination of private keys, is necessary to control and dispose of Ecoterra stored in your digital wallet or vault. Accordingly, loss of requisite private key(s) associated with your digital wallet or vault storing Ecoterra will result in loss of such Ecoterra. Moreover, any third party that gains access to such private key(s), including by gaining access to login credentials of a hosted wallet service you use, may be able to misappropriate your Ecoterra. Any errors or malfunctions caused by or otherwise related to the digital wallet or vault you choose to receive and store Ecoterra, including your own failure to properly maintain or use such digital wallet or vault, may also result in the loss of your Ecoterra. Additionally, your failure to precisely follow the procedures set forth for buying and receiving Ecoterra, including, for instance, if you

provide an incorrect Ecoterra Receipt Address, or provide an address that is not ERC-20 compatible, may result in the loss of your Ecoterra.

Risks of Attacks

As with other decentralized cryptographic tokens based on the Polygon Blockchain, the Tokens are susceptible to attacks in the course of validating Token transactions on the Polygon Blockchain, including, but not limited to, double-spend attacks, majority power attacks, and selfish attacks. Any successful attacks present a risk to the ecosystem and the Tokens, including, but not limited to, accurate execution and recording of transactions involving Tokens.

Risks of Hacking. Security Issues

Hackers or other malicious groups or organizations may attempt to interfere with the Ecosystem or the Tokens in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, smurfing and spoofing. Furthermore, because the Ecosystem is based on open-source software, there is a risk that a third party or a member of the Ecoterra team may intentionally or unintentionally introduce weaknesses into the core infrastructure of the Ecosystem, which could negatively affect the Ecosystem and the Tokens, including the utility of the Tokens for obtaining Services.

Risks of Theft

Ecoterra will make every effort to ensure that the cryptocurrency funds received from the Token Launch will be securely held in the Escrow Wallet. Notwithstanding such security measures, there is no assurance that there will be no theft of the cryptocurrencies as a result of hacks, sophisticated cyber-attacks, distributed denials of service or errors, vulnerabilities or defects on the Website, in the smart contracts on which the Escrow Wallet and the Token Launch rely, on the Polygon Blockchain or any other blockchain, or otherwise. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. In such event, even if the Token Launch is completed, Ecoterra may not be able to receive the cryptocurrencies raised and may not be able to utilize such funds for the development of the Ecosystem. As such, distributed Ecoterra may hold little worth or value, and this would impact its trading price.

Risks Associated with Markets for Tokens

The Tokens are intended to be used solely within the Ecosystem and Ecoterra will not support or otherwise facilitate any secondary trading or external valuation of Tokens. This restricts the contemplated avenues for using Tokens to the provision or receipt of Services, and could therefore create illiquidity risk with respect to any Tokens you own. Even if secondary trading of Tokens is facilitated by third-party exchanges, such exchanges may be relatively new and subject to little or no regulatory oversight, making them more susceptible to fraud or manipulation.

Furthermore, to the extent that third parties do ascribe an external exchange value to Tokens (e.g., as denominated in a digital or fiat currency), such value may be extremely volatile and diminish to zero.

Risks of Future Sales. Issuance of Token

Future sales or issuance of Ecoterra could materially and adversely affect the market price of Ecoterra. Any future sale or issuance of Ecoterra would increase the supply of Ecoterra in the market and this may result in a downward price pressure on Ecoterra. The sale or distribution of a significant number of Ecoterra outside of the Token Launch (including but not limited to the sales of Ecoterra undertaken after the Token Launch, issuance of Ecoterra to persons other than Participants for purposes of community initiatives, business development, education and market expansion and issuance of Ecoterra as a reward to users of the Ecosystem), or the perception that such further sales or issuance may occur, could adversely affect the trading price of the Tokens.

Risks of Uninsured Losses

Unlike bank accounts or accounts at some other financial institutions, Tokens are uninsured unless you specifically obtain private insurance to insure them. Thus, in the event of loss or loss of utility value, there is no public insurer or any private insurance arranged by Ecoterra, to offer recourse to you.

Risks Arising from Taxation

The tax characterization of Tokens is uncertain. You must seek your own tax advice in connection with purchasing Tokens, which may result in adverse tax consequences to you, including withholding taxes, income taxes and tax reporting requirements.

Risks of Competing Ecosystems

It is possible that alternative Ecosystems could be established that utilize similar protocols underlying the Ecosystem and attempt to facilitate services that are materially similar to the Services. The Ecosystem may compete with these alternatives, which could negatively impact the Ecosystem and Tokens, including the utility of the Tokens for obtaining Services.

Risks of Insufficient Interest in the Ecosystem

It is possible that the Ecosystem will not be used by a large number of individuals, companies and other entities or that there will be limited public interest in the creation and development of distributed Ecosystems (such as the Ecosystem) more generally. Such a lack of use or interest could negatively impact the development of the Ecosystem and therefore the potential utility of the Tokens, including the utility of the Tokens for obtaining Services.

Risks Associated with the Development and Maintenance of the Ecosystem

The Ecosystem is still under development and may undergo significant changes over time. Although we intend for the Tokens and Ecosystem to function as described in the Whitepaper and intend to take commercially reasonable steps toward those ends, we may have to make changes to any timelines announced in the Whitepaper, on the Website or any other official channel of Ecoterra, or the specifications of the Tokens or Ecosystem for any number of legitimate reasons. This could create the risk that the Tokens or Ecosystem, as further developed and maintained, may not meet your expectations at the time of purchase.

Risk of Dissolution of Ecoterra or the Ecosystem

It is possible that, due to any number of reasons, including, but not limited to, an unfavorable fluctuation in the value of BTC, ETH, (or other cryptographic and fiat currencies), decrease in the Tokens' utility (including their utility for obtaining Services), the failure of commercial relationships, intellectual property ownership challenges, insolvency, or the liquidation of Ecoterra, the Ecosystem may no longer be viable to operate. The Participants may lose parts or all of their Ecoterra purchasing price.

Risks Arising from Lack of Governance Rights

Because Tokens confer no governance rights of any kind with respect to the Ecosystem or Ecoterra, all decisions involving Ecoterra's products or services within the Ecosystem or Ecoterra itself will be made by Ecoterra at its sole discretion, including, but not limited to, decisions to discontinue its products or services, to create and sell more Tokens for use on the Ecosystem, or to sell or liquidate Ecoterra. These decisions could adversely affect the Ecosystem and the utility of any Tokens you own, including their utility for obtaining Services.

Risks Relating to the Business Partners

Especially at the start, Ecoterra relies on business partners to provide certain Services, especially for Services that require licenses as financial service institutions. While we have legally-binding agreements with business partners and are already in talks with further potential partners, we cannot guarantee that business partners won't terminate their cooperation for whatever reason or that we can close new agreements with potential partners. The provision of certain Services might therefore be interrupted, delayed or cannot be offered at all.

Risks Associated with Markets for Ecoterra

The Ecoterra token is intended to be used solely on the Ecosystem, and Ecoterra will not support or otherwise facilitate any secondary trading or external valuation of Ecoterra. This restricts the contemplated avenues for using Ecoterra to obtain Services or access the Ecosystem, and could therefore create illiquidity risk with respect to Ecoterra you hold. Even if secondary trading of Ecoterra is facilitated by third party exchanges, such exchanges may be relatively new and subject to little or no regulatory oversight, making them more susceptible to market-related risks.

Furthermore, to the extent that third-parties do ascribe an external exchange value to Ecoterra (e.g., as denominated in a digital or fiat currency), such value may be extremely volatile and diminish to zero.

Risks of Data Centre Facilities of Third Parties

Ecoterra's infrastructure is established through servers that it rents at data center facilities of third parties. If Ecoterra is unable to renew its data facility lease under commercially reasonable terms or at all, Ecoterra may be required to transfer its servers to a new data center facility, and may incur significant costs and possible service interruption in connection with the relocation. These facilities are also vulnerable to damage or interruption from, among others, natural disasters, arson, terrorist attacks, power losses, and telecommunication failures. Additionally, the third-party providers of such facilities may suffer a breach of security as a result of third-party action, employee error, malfeasance or otherwise, and a third party may obtain unauthorized access to the data in such servers. As techniques used to obtain unauthorized access to, or to sabotage systems change frequently and generally are not recognized until launched against a target, Ecoterra and the providers of such facilities may be unable to anticipate these techniques or to implement adequate preventive measures. Any such security breaches or damages which occur which impact upon Ecoterra's infrastructure network and/or the Ecosystem may adversely impact the price of Ecoterra.

Risks of Economic Conditions

Ecoterra has been and could continue to be affected by general global economic and market conditions. Challenging economic conditions worldwide have from time to time, contributed, and may continue to contribute, to slowdowns in the information technology industry at large. Weakness in the economy could have a negative effect on Ecoterra's business, operations and financial condition, including decreases in revenue and operating cash flows. Additionally, in a down-cycle economic environment, Ecoterra may experience the negative effects of increased competitive pricing pressure and a slowdown in commerce and usage of the Ecosystem. Suppliers on which Ecoterra relies for servers, bandwidth, location and other services could also be negatively impacted by economic conditions that, in turn, could have a negative impact on Ecoterra's operations or expenses. There can be no assurance, therefore, that current economic conditions or worsening economic conditions or a prolonged or recurring recession will not have a significant adverse impact on Ecoterra's business, financial condition and results of operations and hence the Ecosystem, which would correspondingly impact the trading price of Ecoterra.

Unanticipated Risks

Cryptographic tokens such as Ecoterra are a new and untested technology. In addition to the risks included in this Annex. there are other risks associated with your purchase, possession, and use

of the Tokens, including unanticipated risks. Such risks may further materialize as unanticipated variations or combinations of the risks discussed in this Annex.

Reporting a Security Issue

In case of any security issue is identified, you are required to send us an email to: …….

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 Ecoterra Token and its users.

Please do:

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

Ecoterra 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 Ecoterra 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 Ecoterra 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

Contact Us

Get in touch with us, 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 Ecoterra 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.