TERMS AND CONDITIONS

PHOENIX DAO LLC

[LAST UPDATED ON: 24th February, 2026]

These Terms and Conditions ("**Terms**") constitute a legally binding agreement between the user ("**User**", "**you**") and **Phoenix DAO LLC**, a limited liability company duly organized and existing under the laws of the Republic of the Marshall Islands, together with its affiliates and subsidiaries worldwide (the "**Company**", "**we**", "**us**", **or** "**our**"); it is committed to respecting user privacy and maintaining strong security standards, technical transparency, and responsible protocol stewardship. The Company develops and operates access points and reference implementations for the financial privacy protocol deployed on the Solana blockchain ("**Umbra**" or "**Protocol**"). The Company provides access to a suite of non-custodial privacy-preserving tools, including the web-based interface available at https://umbraprivacy.com/ (the "**Website**"), dashboard related user interfaces, APIs, decentralized applications, mobile integrations, and any associated or successor software, sites, systems, or services (collectively, the "**Platform**").

By accessing, interacting with, or using the Services in any manner, including by connecting a wallet, submitting a transaction, selecting a Relayer, or clicking "**Accept**" or similar acknowledgment, you expressly:

- confirm that you have read, understood, and agreed to be bound by these Terms;
- represent and warrant that you have the legal capacity and authority to enter into these Terms; and
- agree that such acceptance creates a binding contract between you and the Company under the laws of the Republic of the Marshall Islands.

If you do not agree to these Terms, you must immediately discontinue use of the Services.

If you are accepting these Terms on behalf of a company, organization, or other legal entity, you represent and warrant that you have full authority to bind such entities to these Terms. In such circumstances, references to "**you**" or "**your**" shall refer to that entity. If you do not possess such authority, or if you do not agree to all of these Terms, you must not access or use the Services. These Terms, together with the Privacy Policy available at https://d1aj8l6zhs2yl1.cloudfront.net/Umbra-Privacy-Policy-AA160226.pdf and any additional policies, notices, or guidelines issued by the Company from time to time, constitute the entire agreement between you and the Company with respect to your access to and use of the Platform, and Services, and supersede all prior or contemporaneous understandings or agreements, whether

written or oral. The Company may suspend, restrict, or interrupt access to the Platform or Services for scheduled or unscheduled maintenance, security remediation, upgrades, improvements, or technical reasons. Although the Company will use reasonable efforts to minimize disruption, it does not guarantee advance notice and shall not be liable for any consequences of such suspension or interruption. The failure or delay by the Company to enforce any provision of these Terms will not constitute a waiver of that provision or of any other rights, unless such waiver is expressly made in writing by an authorized representative of the Company. If any provision of these Terms is held invalid or unenforceable by a competent tribunal, the remaining provisions shall remain in full force and effect. You may not assign, transfer, or delegate any rights or obligations under these Terms without the Company's prior written consent. The Company may assign or transfer its rights or obligations under these Terms to an affiliate or successor without restriction.

Nothing in these Terms shall be construed to create or imply any partnership, joint venture, employment, fiduciary, or agency relationship between you and the Company. Neither party has authority to bind or obligate the other in any manner except as expressly provided in these Terms.

DEFINITIONS

"Relayer" means an independent off-chain system or operator that, at a User's request, submits a fully authorized blockchain transaction and fronts applicable network transaction fees, without discretion to modify, redirect, approve, or reject transaction contents or access User funds.

"Indexer" means off-chain, read-only software that observes and organizes publicly available blockchain data for informational and usability purposes only.

"Interface-Level Controls" means automated, objective mechanisms that affect routing, prioritization, or visibility of Relayers within Umbra-operated interfaces without affecting transaction validity, authorization, custody, or asset ownership.

1. **INTERPRETATION**
   1.1. ***Modifications***: We reserve the right to change or modify these Terms at any time and at our sole discretion by posting a notification on the Platform. Any changes to or modifications of these Terms will be in effect as of the "Last Updated Date" referred to at the top. You should review these Terms before accessing the Platform. You agree and understand that by accessing the Platform after the "Last Updated Date", you accept and agree to the revised Terms.
   1.2. ***Comprehensive Agreement***: These Terms, along with the Privacy Policy available at: https://d1aj8l6zhs2yl1.cloudfront.net/Umbra-Privacy-Policy-AA160226.pdf (the **"Privacy Policy"**) and any rules outlined on the Platform, constitute a legally binding and enforceable agreement between the Company and you, as an end-user of the Platform. These Terms

supersede any prior or contemporaneous negotiations, discussions, agreements, understandings, representations, and warranties, whether written or oral, between you and us regarding the subject matter.

1.3. ***Headings***: The headings and subheadings in the Terms are for ease of reference only and are not to be taken into account in the construction or interpretation of any provision or provisions to which they refer.

1.4. ***Extended meaning***: Unless otherwise specified in these Terms, words importing the singular include the plural and vice versa and words importing gender include all genders. The word "**include**", "**includes**" or "**including**" will be interpreted on an inclusive basis and be deemed to be followed by the words "**without limitation**".

The language in these Terms will be interpreted as to its fair meaning, and not strictly for or against any party.

2. ELIGIBILITY

2.1. You must be of legal age in your jurisdiction and capable of forming a legally binding contract. Users lacking legal capacity must not access or use the Platform.

2.2. Access is permitted only from jurisdictions where the use of privacy-enhancing blockchain technologies is lawful. You may not use the Platform if it would require the Company to obtain licenses, authorizations, or registrations under local laws.

2.3. You must not be located in, ordinarily reside in, or access the Platform from a jurisdiction subject to international sanctions. You must not be a person or entity subject to sanctions administered by OFAC, EU, UN, or equivalent authorities.

2.4. You are eligible to use the Platform only if you access and interact with it using self-custodied wallets that you control. The Platform is intended only for Users capable of managing private keys, wallets, and blockchain transaction submissions securely.

2.5. Eligibility requires sufficient familiarity with blockchain systems, including the ability to evaluate and manage risks relating to irreversible transactions, gas/network fees, Relayer execution mechanisms, and loss of access to private keys or wallet credentials.

2.6. Eligibility to use the Platform requires consent to electronic terms and enforcement through digital signatures and wallet-based authorization.

2.7. Eligibility requires that use of the Platform comply with applicable financial, AML/CFT, tax, and privacy laws in the User's jurisdiction.

2.8. The Platform is non-custodial and is available only to Users who have the technological ability to self-manage digital assets without custodial support.

3. ABOUT THE PLATFORM

Umbra is a privacy-first transaction protocol on the Solana blockchain that enables users to move digital assets without exposing transactional relationships on-chain. The Protocol is built to restore confidentiality to on-chain value flows by combining shielded commitments, encrypted balances, and zero-knowledge authorization into a single, unified system that remains programmable, composable, and permissionless.

At its core, Umbra allows users to route value through a unified mixer pool, creating cryptographic commitments that decouple senders from recipients. These commitments can later be claimed in multiple ways, giving users direct control over how much information is revealed on-chain. Users may claim value to a public balance, where the total claimed amount is visible, or to a confidential balance, where transaction amounts remain encrypted. In both cases, the recipient address is visible at the time of claim, while sender identity and transaction linkage remain concealed. During commitment creation, sender addresses may be visible, while recipient information is cryptographically hidden.

Umbra introduces a hybrid UTXO and account-based execution model. Value initially exists as UTXO-style commitments inside the shielded pool, enabling strong disassociation. Upon claim, value can transition into standard Solana account balances or encrypted token accounts, allowing users to seamlessly move between private transfers and public on-chain activity without leaving the protocol or fragmenting liquidity.

All interactions with Umbra occur through standard Solana addresses and wallet-signed transactions executed directly against autonomous smart contracts. The Protocol is fully non-custodial: Umbra does not hold user assets, control funds, or act on behalf of users. Transaction initiation, authorization, and key management remain entirely with the user, and no component of the Protocol has the technical ability to access or move user assets unilaterally.

Privacy in Umbra is default, not optional. At the same time, the Protocol supports selective transparency through user-controlled disclosure mechanisms, enabling users to voluntarily reveal transaction data or balances when required for audit, compliance, or reporting purposes. Umbra does not maintain global or master viewing keys and has no inherent access to confidential transaction data.

Umbra operates as an open, permissionless protocol. Independent third-party infrastructure participants, including Relayers, may assist with transaction submission under explicit user authorization, improving usability without

compromising privacy or custody. Any interface-level controls applied to access or routing are automated, objective, and do not alter the non-custodial or permissionless nature of the Protocol.

4. SERVICES AND FUNCTIONALITY

4.1. Platform Services

The Platform provides non-custodial technical interfaces enabling Users to interact with the Umbra Protocol smart contracts deployed on the Solana blockchain. The Platform facilitates access to the Protocol's privacy-preserving functionality without taking custody of assets, managing private keys, or executing transactions on behalf of Users.

Platform services may include, without limitation:

4.1.1. wallet-based connection and transaction signing;
4.1.2. deterministic generation of auxiliary keys including but not limited to shielded private key and master viewing keys;
4.1.3. construction of transactions interacting with the unified shielded pool;
4.1.4. deposit of supported digital assets into the Protocol;
4.1.5. submission of claim transactions utilizing zero-knowledge authorization;
4.1.6. optional routing of transactions through independent Relayers;
4.1.7. viewing and management of encrypted token balances; and
4.1.8. informational dashboards, monitoring tools, and protocol-related analytics.

The Platform acts solely as an access layer and does not modify, approve, or guarantee any on-chain transaction outcome.

4.2. Wallet-Based Access and On-Chain Interaction

4.2.1. Users access and interact with the Platform by connecting a compatible, self-custodied Solana wallet.
4.2.2. No user registration, email address, or credential submission is required.
4.2.3. All actions are executed through digitally signed blockchain transactions.
4.2.4. The Company does not take custody of User assets or manage private keys.

4.3. Privacy Functionality

The Platform enables Users to utilize Umbra's privacy-enhancing features, which include:

a) creation of cryptographic commitments representing value deposited into a unified shielded pool;

b) confidential balance storage through encrypted token accounts;

c) fully private transfers that break on-chain deposit/claim linkages;

d) voluntary opt-in viewing key functionality for auditability.

4.4. Relayer Assistance

4.4.1. The Protocol supports optional Relayer-assisted execution for private withdrawal transactions.

4.4.2. Users may route transactions to an independently operated Relayer to abstract transaction fees and prevent linkage between sending and receiving addresses.

4.4.3. Relayers operate independently and are not custodians, agents, or service providers of the Company or the DAO. While Relayers may be surfaced or routed through Umbra-operated interfaces, the Company and the DAO do not control transaction contents, execution, or asset custody.

4.4.4. The company does not guarantee Relayer availability, uptime, solvency, responsiveness, execution timing, or successful settlement.

4.4.5. A Relayer's refusal, inactivity, failure, or non-responsiveness may prevent successful withdrawal execution and may result in inability to access committed assets.

4.4.6. The Platform may apply automated, objective, and non-discretionary criteria to determine the routing, prioritization, visibility, or availability of Relayers within Umbra-operated interfaces. Such criteria may include sanctions indicators, technical conformance, reliability metrics, abuse prevention signals, and protocol integrity protections. These measures operate solely at the interface or routing level and do not affect the validity, authorization, or execution of transactions submitted directly to the blockchain.

4.4.7. Except where required by applicable law or protocol integrity protections, Relayer controls are implemented through score-based or preference-based routing rather than binary exclusion. Relayers may be deprioritized or omitted from default interface presentation without being blocked from independent operation or direct blockchain interaction.

4.5. Permissionless And Pseudonymous Access

4.5.1. The Protocol's core smart contracts operate without identity-based onboarding or custody; however, access to certain interfaces, execution pathways, or Relayer routing options may be subject to automated Interface-Level Controls without affecting permissionless on-chain interaction.

4.5.2. Users retain control over pseudonymous identifiers (wallet addresses).

4.5.3. The Company cannot recover lost wallet access or reverse executed transactions.

4.6. Smart Contract Execution

4.6.1. All execution is governed by autonomous smart contracts deployed to Solana.

4.6.2. Smart contracts execute deterministically and cannot be reversed once confirmed.

4.6.3. The Company does not control or intervene in validator behavior or blockchain settlement processes.

4.7. Fees and Protocol Charges

4.7.1. The Protocol may impose protocol-level or interface-level fees, which may include fees on deposits into privacy pools, private transactions (including transfers or swaps), and withdrawals back to public addresses. Such fees may vary and are disclosed through the Platform interface at the time of use.

4.7.2. Fees are assessed solely for use of the Protocol and do not constitute custody fees, execution guarantees, performance guarantees, or service-level commitments. No account creation fees are charged.

4.7.3. Any fees generated by the Protocol accrue to the protocol treasury or decentralized governance mechanisms and do not create any fiduciary, agency, or service obligation between the User and the Company.

4.8. Indexers

4.8.1. Indexers are off-chain, read-only systems that organize publicly available blockchain data for usability purposes only. Indexers do not submit transactions, verify proofs, control execution, or affect asset ownership. Indexer availability, completeness, and accuracy are not guaranteed, and Users may independently operate their own Indexers.

5. USER INTERACTION WITH THE PROTOCOL

This section summarizes, at a high level, the operational sequence for interacting with the Umbra Protocol. It is provided for conceptual clarity only and does not modify any other obligations or disclaimers contained in these Terms.

5.1. Wallet Connection

Users interact with the Protocol by connecting a compatible, self-custodied Solana wallet through the Frontend or by programmatic means. No account registration, personal identifiers, or custodial credentials are required. All

actions are authorized exclusively through cryptographic signatures generated by the User's wallet. The Company does not access, store, or control private keys.

5.2. Deposit into the Shielded Pool

To initiate privacy-preserving activity, Users submit deposit transactions to the shielded pool. For each deposit: (a) a cryptographic commitment to encrypted transaction data is recorded on-chain; (b) a nullifier is generated to prevent double-spending; and (c) a Merkle tree leaf is appended to a shared protocol state. The Protocol does not associate deposits with User identity, wallet addresses, or off-chain identifiers.

5.3. Auxiliary Key Derivation and Local Key Management

5.3.1. The Protocol requires Users to derive and manage certain auxiliary cryptographic keys in addition to their primary Solana wallet signing keypair. These auxiliary keys are generated locally by the User and are used to enable privacy-preserving functionality within the Protocol.

5.3.2. Such auxiliary keys may include, without limitation:

5.3.2.1. master viewing or disclosure keys used for optional selective transparency;

5.3.2.2. private keys or secrets used to construct or spend shielded commitments; and

5.3.2.3. cryptographic material required for encrypted balance management and zero-knowledge authorization.

5.3.3. All auxiliary keys are derived and controlled solely by the User. The Company and the Protocol do not generate, store, recover, escrow, or manage auxiliary keys on behalf of Users and do not have access to such keys at any time. Loss, compromise, or misuse of auxiliary keys may result in loss of access to confidential balances, inability to prove entitlement to committed assets, or permanent loss of funds.

5.3.4. Auxiliary keys are distinct from, and do not replace, the User's primary Solana wallet signing keys. All on-chain transactions remain authorized using standard Solana wallet signatures.

5.4. Zero-Knowledge Withdrawal Authorization

To transfer assets out of the shielded pool, Users generate zero-knowledge proofs demonstrating entitlement to encrypted balances without revealing sender, recipient, amount, or transaction history. Upon successful verification:

5.4.1. proof validity is cryptographically verified;

5.4.2. nullifier uniqueness is enforced; and

5.4.3. encrypted balances are updated using decentralized multiparty computation.

State transitions are final once confirmed on the Solana blockchain.

5.5. Relayer-Mediated Transaction Submission

For technical and privacy-preserving reasons, certain Protocol interactions require transaction submission through a Relayer.

In such cases:

5.5.1. the User constructs, authorizes, and cryptographically signs the transaction locally;

5.5.2. the Relayer broadcasts the fully authorized transaction to the Solana network;

5.5.3. applicable network fees are fronted by the Relayer; and

5.5.4. any reimbursement, where applicable, is executed programmatically according to Protocol logic.

Relayers do not custody funds, modify transactions, determine recipients, or control execution outcomes. Relayer availability, responsiveness, or continuity is not guaranteed and may affect the ability to complete certain Protocol actions.

5.6. Encrypted Balance Update

Following each valid deposit or claim, Users' encrypted balances are:

5.6.1. updated autonomously through cryptographic verification and smart contract execution;

5.6.2. stored deterministically within program-derived addresses associated with the User's Solana address; and

5.6.3. publicly readable as encrypted ciphertext by any party capable of querying the blockchain.

Encrypted balances cannot be decrypted without possession of the corresponding decryption key material. Only the User who controls the relevant private decryption keypair is able to decrypt, interpret, or reconstruct the underlying balance amounts.

At no time does the Company, the Protocol, or any Relayer possess the ability to decrypt encrypted balances, view underlying amounts, or access User financial data absent User-controlled disclosure.

6. RELAYER, AUTOMATION, ROUTING AND INTERFACT CONTROLS

6.1. Core Principle

Relayer-related automation operates exclusively at the interface and routing level and does not affect transaction validity, authorization, execution, custody, or asset ownership. No automation implemented by the Company, the DAO, or the Protocol shall:

a) freeze, seize, restrict, or take custody of User funds;
b) invalidate, reverse, or modify blockchain transactions; or
c) require human approval for transaction execution.

Automation may only determine whether and how Relayers are surfaced, deprioritized, or excluded within Umbra-operated interfaces.

6.2. Automated Relayer Control Model

For technical, privacy-preserving, or protocol-integrity reasons, certain actions (including private withdrawals, claims, or other shielded operations) require Relayer-mediated submission. Users acknowledge and accept that:

a) inability or refusal of a Relayer to submit a transaction may delay or prevent execution;
b) Relayer unavailability may result in temporary or permanent inability to perform certain Protocol actions; and
c) such limitations do not constitute freezing, seizure, or custody of User assets.

Ownership of assets remains with the User at all times, notwithstanding execution dependencies.

6.3. Interface Control

Relayer selection, routing, and availability within Umbra-operated interfaces may be governed by automated, objective, and non-discretionary mechanisms. Such mechanisms operate solely at the interface and routing level and may consider:

a) legal or sanctions-related risk indicators;
b) technical conformance and protocol-integrity requirements;
c) performance, availability, or reliability metrics; and
d) abuse prevention or network-safety protections.

These mechanisms do not affect transaction validity, authorization, cryptographic correctness, or asset ownership.

6.4. Interface Level Measures

In exceptional circumstances involving active exploitation, systemic protocol risk, or legal compulsion, temporary interface-level restrictions may be applied to Relayer routing, as further detailed in the Relayer Standard and Eligibility Policy (insert link of the Policy). Such measures are:

(a) limited to routing and interface availability;
(b) time-bound and subject to automatic expiration; and
(c) without effect on transaction validity, smart contract logic, or User asset ownership.

6.5. Relayers do not act as agents, custodians, fiduciaries, or service providers of the Company or the DAO. The Company and the DAO do not guarantee Relayer availability, uptime, responsiveness, or execution success. Users assume all risks associated with mandatory reliance on Relayer-mediated transaction submission.

7. ELECTRONIC CONSENT AND WALLET BASED AUTHORIZATION

7.1. You acknowledge and agree that your access to and use of the Platform is conditioned upon your electronic acceptance of these Terms. For purposes of applicable contract, electronic transactions, and evidence laws, including without limitation the Electronic Transactions Act (Marshall Islands) and analogous laws in other jurisdictions, you expressly agree that:

7.1.1. **Wallet Signatures as Legal Consent.** Any cryptographic signature, message signing, or transaction authorization executed using a blockchain wallet that you control constitutes your valid and binding electronic signature, and has the same legal effect as a handwritten signature or written consent.

7.1.2. **On-Chain Actions as Acceptance.** Your use of the Platform, including but not limited to connecting a wallet, submitting transactions, signing messages, interacting with smart contracts, depositing assets, generating proofs, selecting Relayers, or otherwise invoking Protocol functionality, constitutes your affirmative acceptance of, and agreement to be legally bound by, these Terms, as amended from time to time.

7.1.3. **Irrevocability of Blockchain Authorization.** You acknowledge that blockchain-based authorizations and transactions, once signed and submitted, are technically irreversible and may not be withdrawn, revoked, or rescinded, and you agree that such authorizations evidence your intent to be legally bound at the time of execution.

7.1.4. **No Additional Formalities Required.** You waive any requirement for physical signatures, paper records, or additional confirmations, and agree that no further action, acknowledgment, or documentation is required to establish the enforceability of these Terms.

7.1.5. **Attribution.** All wallet-based actions and signatures are deemed to be performed by you and attributable to you, whether initiated directly or indirectly through software, interfaces, APIs, or Relayers, and you accept full responsibility for such actions.

8. INTELLECTUAL PROPERTY

8.1. All rights, title, and interest in and to the Platform, the Umbra Protocol reference implementations, and all associated materials, including but not limited to software code, smart contracts, cryptographic designs, algorithms, system architecture, interface components, documentation, trademarks, trade names, service marks, logos, UI/UX layouts, and any related content or proprietary materials (collectively, "**Intellectual Property**") are and shall remain the exclusive property of the Company, its contributors, or its licensors.

8.2. This includes any upgrades, improvements, bug fixes, patches, parameter changes, or derivative works, whether developed internally or arising from User feedback or community suggestions. Nothing in these Terms shall be construed as granting you any rights or interests in such Intellectual Property other than the limited license expressly permitted herein.

8.3. Subject to compliance with these Terms, the Company grants you a limited, revocable, non-exclusive, non-transferable, non-sublicensable license to access and use the Platform solely for lawful, personal, and non-commercial purposes connected with interacting with the Umbra Protocol. This limited license does not permit:

8.3.1. reproduction, modification, redistribution, public display, or commercial use of any part of the Platform; or

8.3.2. using the Platform for illegal, unauthorized, or exploitative purposes.

8.4. You shall not, and shall not assist or permit any third party to:

8.4.1. copy, replicate, modify, translate, or create derivative works based on the Platform or protocol code;

8.4.2. reverse-engineer, decompile, or attempt to extract source code from the Platform, smart contracts, cryptographic components, or related software;

8.4.3. remove, obscure, or modify proprietary notices or branding;

8.4.4. scrape, harvest, or extract content or data from the Platform without written authorization;

8.4.5. commercially exploit any Intellectual Property without prior written consent from the Company.

Any unauthorized use constitutes a material breach of these Terms.

8.5. All names, logos, and branding associated with "**Phoenix**," "**Umbra**," the Umbra Protocol, and other marks displayed on the Platform are trademarks or service marks owned by the Company or its licensors. Nothing herein grants any license or right to use such marks, and unauthorized use may constitute trademark infringement.

8.6. If you provide the Company with suggestions, enhancements, feature ideas, bug reports, or other feedback (**"Feedback"**), you acknowledge and agree that such Feedback is provided voluntarily and without confidentiality obligations. You grant the Company a perpetual, irrevocable, worldwide, royalty-free license to use, reproduce, disclose, and incorporate such Feedback into the Platform or related projects without obligation or compensation to you.

G. THIRD PARTY SERVICES

G.1. The Platform may provide access to, integrate with, or rely on third-party tools, networks, wallets, Relayers, Multi-Party Computation (MPC) nodes, cryptographic libraries, RPC infrastructure, indexers, explorers, or other decentralized or traditional services. Such references or integrations do not constitute endorsement, control, or responsibility by the Company.

G.2. Use of third-party services, including independent Relayers operating outside the Company control, is entirely at your own risk. The Company is not responsible for:

- 9.2.1. degradation or denial of service by Relayers or RPC providers;
- 9.2.2. bugs, failures, exploits, or interruptions in third-party software;
- 9.2.3. misleading or inaccurate information provided by external sources;
- 9.2.4. withdrawal or refusal of a Relayer to execute a claim transaction.

10. USER REPRESENTATIONS AND WARRANTIES

By accessing or using Umbra, including any smart contracts, shielded pools, Relayer interfaces, SDKs, program-derived addresses, key management modules, or related applications, you represent and warrant that:

10.1. You understand and accept the inherent risks associated with interacting with blockchain networks, cryptographic protocols, encrypted balance systems, MPC infrastructure, and privacy-preserving Relayers.

10.2. You will use the Protocol only for lawful purposes and in full compliance with applicable laws and regulations, including sanctions, AML, tax, reporting, and privacy laws.

10.3. You will not interact with the Protocol if you are a resident, national, or entity located in a jurisdiction where the use of privacy-preserving cryptographic systems, mixers, Relayers, or decentralized asset transfers is prohibited or restricted.

10.4. You represent that you are at least the age of majority in your jurisdiction and have capacity to enter into these Terms.

10.5. All information, authorizations, or credentials you provide in connection with your use of the Protocol are accurate and complete.

10.6. You acknowledge that Umbra is a decentralized, non-custodial protocol and does not control, hold, or recover private keys, balances, encrypted states, viewing keys, or other user credentials.

10.7. You acknowledge that Umbra does not act as a broker, custodian, financial institution, payment processor, or regulated service provider.

10.8. You will not attempt to exploit, attack, compromise, or interfere with any cryptographic mechanism, MPC computation, ZK proof generation/verification, Relayer execution flow, or shielded pool logic.

10.G. You will promptly and responsibly disclose any discovered bugs, vulnerabilities, or suspected exploits to the Umbra development contributors at legal@umbraprivacy.com.

10.10. You acknowledge that Umbra contributors, developers, and affiliates do not guarantee continued availability, liveness, or execution finality of the Protocol.

11. DISCLAIMER OF WARRANTIES

The platform is provided on an **"as-is"** and **"as-available"** basis. To the maximum extent permitted under applicable law, the company and its contributors, developers, affiliates, service providers, and relayers disclaim all warranties, express or implied, including without limitation:

11.1. Warranties of merchantability, fitness for a particular purpose, title, non-infringement, security, or uptime;

11.2. Warranties related to correctness, verifiability, validity, confidentiality, secrecy, or unlinkability of transactions or encrypted balances; and

11.3. Warranties relating to liveness, finality, relayer execution, MPC availability, correct ZK-proof verification, or successful submission/settlement of transactions.

Umbra makes no representation, warranty, or guarantee that:

11.4. the Protocol will be uninterrupted, error-free, secure, private, resistant to analysis, immune from attack, or continuously available;

11.5. encrypted balances will remain confidential, recoverable, or computationally secure in perpetuity;

11.6. Relayers will be available, responsive, live, trustworthy, or capable of completing required transactions;

11.7. MPC nodes, cryptographic primitives, shielded pool mechanisms, or deterministic address derivations will operate correctly or free from compromise;

11.8. ZK proofs, nullifiers, encryption keys, or commitments will remain technically sound or computationally secure;

11.G. the Protocol will function as intended following forks, chain re-organizations, advances in cryptography, quantum breakthroughs, or regulatory intervention.

Your use of the Protocol, encrypted balances, shielded pool, MPC infrastructure, and Relayer execution systems is entirely at your sole risk.

12. USER RESPONSIBILITIES AND RISKS

By accessing or using Umbra, including interacting with its Protocol, including but not limited to the smart contracts, shielded pools, deterministic Solana Addresses, MPC computation network, Relayer infrastructure, SDKs, or related tooling, you agree, acknowledge, represent, and warrant the following:

A. User Responsibilities

12.1. You are solely responsible for all actions taken through any Solana wallet you connect to the Protocol and for securing all associated private keys, seed phrases, viewing keys, master viewing keys, or other credentials. Umbra cannot retrieve, restore, or reset credentials.

12.2. You are fully responsible for the legality of your use of the Protocol, including compliance with any applicable laws governing the sanctions and AML/CFT, reporting, taxation, recordkeeping, data privacy and cryptography, digital asset transfer and money transmission

12.3. You acknowledge that all transactions submitted to the Solana blockchain, including deposits into the shielded pool, claim transactions, state updates, and Relayer-submitted transactions are final, irrevocable, and irreversible. Umbra contributors cannot reverse, unwind, or recover transferred assets.

12.4. You agree not to misuse the Protocol, including attempts to bypass screening controls, access viewing keys of other users, reverse-engineer cryptographic systems, interfere with Relayer execution, or exploit vulnerabilities for personal benefit.

12.5. Continued access to the Protocol is conditioned upon lawful use and compliance with these Terms, and Umbra contributors may restrict access in response to suspected abuse or illegal interactions to the extent technically feasible.

B. Risks

You acknowledge, understand, and agree that your access to and use of the Umbra Protocol, including any associated smart contracts, shielded pools, deterministic Solana Addresses, multi-party computation (MPC) networks, Relayer infrastructure, interfaces, SDKs, cryptographic systems, and related tooling, involves significant technical, operational, and legal risks. You further

acknowledge and agree that all such use is undertaken at your own risk. To the maximum extent permitted by applicable law, neither the Company, the Protocol, nor any of their respective contributors, developers, service providers, affiliates, or infrastructure participants shall be responsible or liable for any loss, damage, delay, inaccessibility, or inability to use the Protocol or any component thereof, except as expressly required by law. These risks include, without limitation, the following categories:

B.1. Technical and Cryptographic Risks

12.6. The Protocol relies on advanced cryptographic constructs, including deterministic key derivation, Program-Derived Addresses (PDAs), Rescue-based encryption, Merkle commitments, nullifiers, multi-party computation (MPC), and zero-knowledge proofs (ZKPs), which remain experimental and may contain undiscovered vulnerabilities.

12.7. Smart contracts may contain defects, bugs, exploits, or vulnerabilities that could result in unauthorized access, loss of funds, or irreversible transaction failures.

12.8. Cryptographic advances or failures including advances in cryptanalysis or computing (e.g., quantum computing) may compromise security guarantees and expose private balances or transaction linkages.

12.G. Network congestion, degraded validator performance, forks, re-orgs, consensus failures, or censorship may delay or prevent execution of deposits, claims, or withdrawals.

B.2. Relayer Execution and Liveness Risks

12.10. Certain Protocol interactions depend on third-party Relayers for execution and fee abstraction; Relayers may experience downtime, unresponsiveness, misconfiguration, or operational issues, users are not restricted to a single Relayer.

12.11. Relayer selection occurs at the time of claim and can be changed if a chosen Relayer is unavailable or non-functional. In the event a Relayer goes offline or fails to execute a transaction, users may temporarily lose the ability to submit a claim but do not lose ownership of their assets. Claims can be routed through an alternative Relayer, or a new Relayer may be deployed, provided it passes the required validation and checks. .

12.12. However, reliance on Relayers introduces operational dependencies that may result in temporary delays or interruptions in execution. Users acknowledge that such dependencies may impact the timing or availability of claims, transfers, or recoveries.

12.13. No contributor or affiliated party is obligated to operate, replace, subsidize, or expedite Relayers, nor to assist in recovery or execution beyond the functionality provided by the protocol.

B.3. Privacy and Confidentiality Risks

12.14. While the Protocol seeks to provide confidentiality, absolute unlinkability or anonymity cannot be guaranteed. Inference attacks, metadata correlation, timing analysis, off-chain identifiers, or cryptographic breakthroughs may compromise privacy.

12.15. Viewing key misuse, compromise, improper storage, or compelled disclosure may allow unauthorized parties to access confidential transaction information or account balances.

B.4. Ownership, Finality, and Loss of Control Risks

12.16. All transactions executed on-chain are final, irreversible, and may not be cancelled, reversed, or restored.

12.17. Loss of access to private keys, derived keys, seeds, wallets, or credentials including for Solana Addresses may result in permanent loss of access to balances, with no recourse or recovery mechanism.

12.18. Protocol-level state transitions and cryptographic commitments are enforced through zero-knowledge proofs. Invalid commitments cannot be submitted, as commitment correctness is enforced within the zk-proof constraints. As a result, users cannot lose assets due to the submission of an invalid commitment at the protocol level.

B.5. Economic and Market Risks

12.1 G. The value of digital assets deposited into or withdrawn from the Protocol may fluctuate, depreciate, or become worthless.

12.20. Use of encrypted/private balances may complicate or impair price discovery, liquidation, accounting, or solvency analysis.

B.6. Legal, Regulatory, and Compliance Risks

12.21. Laws and regulations governing cryptography, mixers, privacy technologies, MPC, ZKPs, Relayers, money transmission, sanctions compliance, data protection, export controls, reporting, and digital assets remain uncertain and rapidly evolving.

12.22. Regulators may classify the Protocol or users' conduct as financial intermediation, VASP/Money Services Business activity, remittance,

custodial service, mixer use, sanction evasion, or other regulated conduct retroactively or in specific jurisdictions.

12.23. Users may incur registration, licensing, disclosure, reporting, tax, or AML/KYC obligations, including obligations related to selective disclosure using viewing keys. The Company does not intentionally collect or process personal data. On-chain data consists of public blockchain addresses, cryptographic commitments, and encrypted metadata, which are not designed to identify natural persons. Such data may, in certain circumstances and when combined with off-chain information, be associated with an identifiable individual; however, the Company does not control such linkage and cannot modify or delete immutable blockchain data.

12.24. Enforcement authorities may seek to compel disclosure of identifiers, viewing keys, metadata, or transactional records and failure to comply may result in legal liability.

12.25. Users risk interacting unknowingly with tainted or illicit funds or sanctioned persons, potentially exposing themselves to seizure, forfeiture, freezing, or enforcement actions.

12.26. Users operating Relayer infrastructure may incur separate licensing, AML, sanctions, or reporting obligations arising from fee abstraction or broadcast services.

12.27. Privacy-enhancing transactions may attract enhanced regulatory or law enforcement scrutiny.

12.28. Conflicts of law among jurisdictions may affect validity, enforceability, or legal recognition of cryptographic transfers, ownership proofs, or finality.

12.2 G. Encrypted balances may complicate future inheritance, insolvency resolution, civil litigation, audits, divorce, bankruptcy, tax investigations, or claims to ownership.

B.7. No Duty, No Guarantee, No Recourse

12.30. The Protocol is experimental and provided on a non-custodial basis.

12.31. No contributor, developer, affiliate, operator, Relayer, or service provider guarantees execution, settlement, continued availability, liveness, balance confidentiality, solvency, or correct functioning of the Protocol.

12.32. No person has any obligation to refund, reimburse, replace, restore access, retrieve balances, or compensate for any loss, delay, error, failure, or unavailability of the Protocol.

B.8. Interface, Frontend, and Dependency Risks

12.33. Users may rely on Umbra-operated interfaces, dashboards, SDKs, APIs, or reference implementations to interact with the Protocol. Such interfaces may

contain bugs, inaccuracies, latency, stale data, misconfigurations, or display errors that do not reflect actual on-chain state.

12.34. Interface availability, correctness, or usability may be affected by software defects, upgrades, browser compatibility, mobile operating systems, third-party dependencies, or infrastructure outages.

12.35. The authoritative record of ownership, balances, and execution is the blockchain itself. The Company does not guarantee that any interface accurately reflects Protocol state at any given time.

B.G. Data Integrity s Indexing Risk

12.36. The Protocol may rely on indexers or off-chain data aggregation systems to present balances, transaction history, or Protocol state. Such systems may be incomplete, inaccurate, delayed, censored, or unavailable.

12.37. Incorrect or missing indexed data may cause Users to make incorrect assumptions regarding balances, execution status, or eligibility, for which the Company bears no responsibility.

B.10. Force Majeure and External Intervention Risks

12.38. Access to or operation of the Protocol may be disrupted or permanently impaired by events beyond the Company's control, including government action, regulatory intervention, sanctions, court orders, infrastructure seizure, internet outages, cloud service termination, or force majeure events.

12.3 G. Such events may result in loss of access, inability to transact, or permanent inaccessibility of balances, without liability to the Company or any contributor.

13. INDEMNITY

13.1. Indemnification by You

To the fullest extent permitted by applicable law, you agree to indemnify, defend, and hold harmless Phoenix DAO LLC, and each of their respective affiliates, contributors, developers, officers, directors, agents, contractors, service providers, infrastructure participants (including Relayer operators and MPC node operators), and representatives (collectively, the **"Umbra Parties"**) from and against any and all claims, demands, actions, proceedings, investigations, inquiries, liabilities, damages, losses, penalties, fines, forfeitures, seizures, costs, and expenses (including reasonable attorneys' fees, expert fees, and enforcement defence costs) arising out of or relating to, directly or indirectly:

13.2. your access to, use of, or interaction with the Protocol, Platform, smart contracts, shielded pools, Solana Addresses, Relayer mechanisms, MPC infrastructure, SDKs, or cryptographic systems;

13.3. any transaction you initiate, authorize, route, or execute, whether directly or through a Relayer;

13.4. any loss, inaccessibility, freezing, seizure, or inability to recover digital assets resulting from protocol design, cryptographic dependencies, Relayer behaviour, or enforcement actions.

13.5. your actual or alleged violation of any applicable law, regulation, or rule, including without limitation laws relating to:

- sanctions, embargoes, or restricted persons (including OFAC, EU, UN regimes);
- anti-money laundering or counter-terrorist financing;
- digital asset transfer, money transmission, or licensing;
- data protection, privacy, or cryptography controls;
- tax, reporting, disclosure, or recordkeeping obligations;
- any enforcement action, investigation, subpoena, seizure, freezing order, forfeiture, or regulatory inquiry arising from your use of the Protocol.
- any act or omission of a Relayer selected or utilized by you, including refusal to act, delay, censorship, mis execution, fee disputes, front-running, metadata exposure, or permanent unavailability;
- any claim asserting that a Relayer acted as an agent, intermediary, service provider, or representative of the Umbra Parties;
- any claim arising from reliance on Relayer-assisted execution, fee abstraction, or gasless transaction routing.
- any compromise, misuse, loss, compelled disclosure, or unauthorized access to viewing keys, master viewing keys, cryptographic secrets, or metadata;
- any claim that privacy guarantees were insufficient, compromised, or invalidated due to inference attacks, regulatory intervention, or technological developments;
- any allegation that the Protocol facilitated concealment, obfuscation, or evasion of monitoring or enforcement.
- any attempt to exploit, reverse-engineer, interfere with, or compromise the Protocol, cryptographic mechanisms, ZK proofs, Relayer flows, MPC processes, or screening safeguards;
- any use of the Protocol to transfer, conceal, launder, or otherwise handle proceeds of unlawful activity.

13.6. The Umbra Parties may, but shall not be obligated to, assume exclusive control of the defence and settlement of any matter subject to indemnification.

You agree to fully cooperate, provide truthful information, and not take any action that would prejudice the Umbra Parties' defence.

13.7. You may not settle any claim, admit liability, or consent to judgment that imposes any obligation, liability, restriction, or admission on any Umbra Party without their prior written consent, which may be withheld in their sole discretion.

13.8. Your indemnification obligations under this Section survive termination, suspension, or cessation of your access to the Protocol or Platform, and apply regardless of fault, negligence, strict liability, or regulatory classification theories asserted against the Umbra Parties.

13.G. Your indemnification obligations survive termination or suspension of access to the Protocol.

14. LIMITATION OF LIABILITY

14.1. To the maximum extent permitted by applicable law, the Umbra Parties shall not be liable to you under any legal or equitable theory, whether in contract, tort (including negligence), strict liability, statute, fiduciary duty, misrepresentation, restitution, or otherwise, for any loss, damage, liability, cost, or expense, arising out of or relating to, directly or indirectly:

(a) your access to, use of, or inability to access or use the Protocol, Platform, or any related smart contracts, cryptographic systems, MPC infrastructure, relayer services, SDKs, interfaces, or documentation;

(b) any reliance upon the Protocol's privacy, confidentiality, anonymity, unlinkability, liveness, execution, availability, recoverability, or security characteristics, whether express or implied;

(c) the performance, non-performance, delay, refusal, unavailability, misconfiguration, compromise, or cessation of any relayer, MPC node, validator, oracle, RPC provider, wallet, or other third-party or decentralized infrastructure component;

(d) any failed, delayed, rejected, incomplete, or erroneous deposit, claim, withdrawal, proof generation, proof verification, nullifier usage, Merkle tree update, encrypted balance update, or transaction of any kind;

(e) loss of access to, or compromise of, wallets, private keys, seed phrases, viewing keys, master viewing keys, derived keys, credentials, or cryptographic material;

(f) blockchain-level events, including but not limited to forks, reorganizations, rollbacks, censorship, validator behaviour, consensus failures, network congestion, or protocol upgrades;

(g) regulatory, enforcement, or judicial actions, investigations, sanctions determinations, compelled disclosures, or changes in law that affect the Protocol or your ability to access or use it; or

(h) any unauthorized access, misuse, exploitation, or attack involving wallets, relayers, MPC nodes, cryptographic systems, or third-party infrastructure.

14.2. Without limiting Section 13.1, in no event shall the Umbra Parties be liable for any damages of any kind, including direct, indirect, incidental, consequential, special, exemplary, or punitive damages, or for any loss of profits, revenue, goodwill, data, privacy, anonymity, digital assets, balances, business opportunity, or economic advantage, even if the Umbra Parties were advised of the possibility of such damages and even if any remedy is alleged to have failed of its essential purpose.

14.3. You expressly acknowledge and agree that:

(a) the Protocol is non-custodial, experimental, and decentralized in nature;

(b) the Umbra Parties do not assume any duty of care, fiduciary obligation, operational responsibility, or guarantee with respect to execution, settlement, confidentiality, recoverability, or continued availability of the Protocol or any associated infrastructure; and

(c) you may have no legal or equitable remedy against the Umbra Parties in the event of loss, delay, unavailability, or failure of any component of the Protocol.

15. TERMINATION AND SUSPENSION

15.1. Access Restriction and Protocol Controls

Umbra reserves the right, to the maximum extent technically feasible and legally required, to suspend or terminate access to the Protocol, including:

15.1.1. denial of deposits at the program level through sanctions or risk screening;

15.1.2. refusal or inability of MPC nodes or Relayers to process claims;

15.1.3. disabling or discontinuing smart contract operations;

15.1.4. network upgrades, migration, maintenance, or deprecation;

15.1.5. suspension in response to legal obligations, enforcement orders, or regulatory inquiries;

15.1.6. detection or suspicion of abuse, unlawful activity, or misuse of cryptography or Relayer infrastructure.

In extraordinary circumstances involving active exploitation, systemic protocol risk, or legal compulsion, temporary interface-level restrictions may be applied to Relayer routing. Such measures are limited in scope, time-bound, and do not affect asset ownership, transaction authorization, or the ability to submit

transactions directly to the blockchain. Emergency controls expire automatically unless extended through decentralized governance.

15.2. Effect of Suspension

Suspension may result in:

15.2.1. inability to perform deposits, claims, withdrawals, or other shielded interactions;

15.2.2. loss of access to balances held within the shielded pool;

15.2.3. delays or indefinite inability to execute transactions requiring Relayers or MPC participation;

15.2.4. no obligation for Umbra Parties to restore access or recover assets.

Suspension does not limit obligations arising prior to the suspension, including indemnification.

15.3. Effect of Termination

Upon termination:

15.3.1. access to the Protocol ceases immediately;

15.3.2. Umbra Parties have no obligation to restore, recover, decrypt, or assist in accessing balances, proofs, or encrypted state;

15.3.3. you remain responsible for obligations accrued before termination.

You may cease use of the Protocol at any time; however, doing so does not release you from obligations incurred prior to discontinuation.

16. GOVERNING LAW AND EXCLUSIVE JURISDICTION

16.1. These Terms and any Dispute shall be governed by and construed in accordance with the laws of the Republic of the Marshall Islands, without regard to any choice-of-law or conflict-of-laws principles that would require application of laws of another jurisdiction.

16.2. Subject to Section 16.3 below, the courts of the Republic of the Marshall Islands shall have exclusive jurisdiction to hear and determine any Dispute. You irrevocably submit to the personal and subject-matter jurisdiction of such courts and waive any objection based on forum non conveniens or lack of jurisdiction.

16.3. Nothing in these Terms shall prevent the Company from seeking interim, injunctive, or equitable relief in any court of competent jurisdiction where necessary to protect the Protocol, cryptographic systems, smart contracts, infrastructure, or intellectual property.