
**SECURITY ALLIANCE (SEAL)
WHITEHAT SAFE HARBOR AGREEMENT
&
RELATED MATERIALS**

v. 1.01

TECHNICAL SUMMARY

OF WHITEHAT SAFE HARBOR AGREEMENT

PLEASE READ ALL OF THE WHITEHAT SAFE HARBOR AGREEMENT (THE “AGREEMENT”) VERY CAREFULLY. THE BULLET POINTS BELOW ARE ONLY A PARTIAL SUMMARY OF SOME OF THE MATERIAL TERMS OF THE AGREEMENT. IN ALL CIRCUMSTANCES, INCLUDING IN THE EVENT OF ANY CONFLICT OR INCONSISTENCY BETWEEN THIS OR ANY OTHER SUMMARY AND THE TEXT OF THE AGREEMENT, THE TEXT OF THE AGREEMENT WILL GOVERN, TO THE EXCLUSION OF THE SUMMARY. CERTAIN TERMS USED IN THIS SUMMARY ARE DEFINED IN THE AGREEMENT. BE RESPONSIBLE AND THOROUGH - FAILING TO FOLLOW THE TERMS OF THE AGREEMENT COULD RESULT IN SERIOUS LEGAL CONSEQUENCES.

MOTIVATION AND BACKGROUND

- The intention of the agreement is to provide a framework that:
 - Rewards whitehats for locating active exploits,
 - Allows whitehats to proactively secure protocol funds, and
 - Protects *responsible* actors against legal risk.
- As a “whitehat,” you should act competently and in good faith.
 - While there is no formal standard of “competence,” a competent whitehat has some background experience in software engineering, security, and/or blockchain auditing.
 - Hacking a protocol affects other people’s money and can have irreversible consequences. Proceed with caution, act ethically, and execute well.
- **Provided that you do act lawfully, competently and in good faith, the protocol and its members waive the right to pursue legal claims against you.** However, be aware that the legal landscape is complex, and engaging in agreements of this nature carries associated risks. Exercise caution and seek advice as necessary.
- If you successfully rescue and return exploited assets to the Asset Recovery Address (ARA) in compliance with the agreement, you may be entitled to a reward (typically proportional to your transfers to the ARA).

CHECKLIST

- In order to abide by the terms of this agreement and be covered by its protections, you must be able to answer “yes” to all of the following:
 - Is this an active, urgent exploit?
 - Are you unable to responsibly disclose the exploit (e.g. via a bug bounty program) due to time constraints or other reasons?
 - Can you reasonably expect your intervention to be net beneficial, reducing total losses to the protocol and associated entities?

- Are you experienced and confident in your ability to manage execution risk, avoiding unintentional loss of funds?
- Will you avoid intentionally profiting from the exploit in any way other than through the reward granted by the protocol?
- Are you and anyone with whom you directly cooperate during the funds rescue, as well as all funds and addresses used in said rescue, free from OFAC sanctions and/or other connections to sanctioned parties?
- Have you confirmed the agreement has been duly adopted by the protocol community?
- Are you fully aware of the risks associated with your actions, including but not limited to accidental loss of funds, claims and liabilities outside this agreement's scope, and the unclear extent of this agreement's enforceability?
- Have you thoroughly read the entire agreement and understand all of its terms and conditions?
- Before executing a funds rescue and/or depositing funds to an ARA, always confirm that the conditions listed above still hold.

THE AGREEMENT

- *Main point:* If you follow this agreement and meet its requirements as a whitehat, the protocol and its users agree not to take legal action against you or raise complaints to the government in connection with your actions under the agreement.
 - The aim of this agreement is to enable rewards for whitehats and provide legal protection for proactively securing funds against active exploits. By adopting it, the protocol gives you the freedom to act in its best interest, in situations where following an ordinary bug-bounty disclosure program may be impossible or impractical.
 - This agreement covers the protocol and its users, but does not (and cannot) cover the actions of government or regulatory entities. You should still proceed with utmost caution.
 - The protocol can change the terms of the agreement at any time prior to an exploit, including what is in or out of scope. It is your responsibility to be aware of the most current version.
- *Exploits:* You may be entitled to a reward for performing a **funds rescue**, which must meet the following conditions.
 - Deposits all tokens removed from the protocol into the ARA, possibly excluding any **retained reward** allowed under the agreement.
 - Addresses an active threat that has already been triggered by someone else. Only *active exploits* are covered - you are not allowed to start the process, but you can finish it. See Section 2 under **urgent blackhat exploits**.
 - Follows the specified process in the agreement, including any addenda.
 - Notifies the protocol as soon as reasonably practicable, such as immediately after the funds rescue is complete. If for any reason you cannot deposit funds to the ARA within 6 hours post-rescue, you must notify the protocol.

- Is performed by whitehats who can make the necessary representations and warranties. If you cooperate with anyone, pick known good actors.
- Note that by default, you are considered a **prospective whitehat** who makes a conscious decision to initiate a rescue. However, if an automated contract (or **generalized arbitrage bot**) owned or operated by you has already performed an exploit, you are instead considered a **retrospective whitehat**, in which case you must notify the protocol and initiate the return of funds once you become aware of the exploit.
- *Expenses and rewards*
 - You are allowed to incur reasonable expenses in the course of the rescue (e.g. gas fees and slippage costs).
 - You should attempt to minimize unnecessary expenses. Don't destroy the value of the assets while saving them.
 - Any proportional reward is calculated based on the US dollar value of the **returnable assets**, equal to the exploited assets minus any funds used in good faith to rescue and deposit those assets. SEAL recommends a 10% Bounty, but the Bounty percentage may be adjusted or capped in a specific protocol agreement.
 - Protocols may also specify an `aggregateBountyCapUSD`, which limits the total bounty payouts across all whitehats for a single exploit. If this cap is exceeded, rewards are reduced proportionally.
 - Your reward is based on the funds you individually secured, and will be transferred by default to the originating address used during the rescue.
- *Receiving rewards:* You may use either of the following two methods.
 - (A) Return all assets to the ARA and specify, through a clearly identifiable public message (e.g. an event or transaction payload), where you wish to receive the reward.
 - (B) Return all assets to the ARA *except* the designated reward. Deposit the reward in an address that you verify in writing to the protocol publicly, as with method (A).
 - In either case, the protocol has 15 days to initiate a dispute. You may presume the reward is accepted unless you are notified otherwise.
- If the protocol decides you've broken the agreement, it can refuse to pay your reward even if you've already completed a funds rescue. If you completed a valid rescue, you may be able to still claim a reward through the dispute resolution process provided in the agreement. For more details, see **dispute resolution**.

COVENANTS YOU ARE AGREEING TO AS A WHITEHAT

- You have read and understood the full agreement (**not just this summary**), including any modifications made by the protocol when adopting the agreement.
- All secondary actions taken in connection with the funds rescue are legal.
- You will follow all necessary precautions to prevent collateral damage. For instance, you will not execute transactions via a public mempool vulnerable to frontrunning or similar forms of interference.
- The protocol is not responsible for monitoring you or ensuring you follow the law.

- Participating does not make you an employee or representative of the protocol, nor does it create any exclusive relationship.
- The reward outlined in the agreement is the only compensation due.
- The protections outlined in the agreement apply only if the protocol agrees that you have not violated its terms.
- Provided you follow the agreement, neither the protocol nor its members may pursue present or future legal claims against you in connection to the funds rescue.
- However, you also waive any claims against the protocol and its members.

REPRESENTATIONS AND WARRANTIES YOU MAKE AS A WHITEHAT

By participating, you assert that all of the following are true:

- You are legally able to enter into this agreement.
- Any blockchain addresses and any additional funds used to perform the rescue are clean, and not obtained illegally or from a sanctioned source.
- You are not currently subject to sanctions from OFAC.
- You are not a senior political official.
- You are not violating any other agreement by participating in this one.
- You have sufficient experience in blockchain security to perform the rescue competently, and have weighed the risks and benefits of doing so.
- You are not currently the target of legal action related to other blockchain exploits.
- You either own or have a valid license for any tools and intellectual property used in the course of the rescue.
- You have not triggered the blackhat exploit yourself (which would nullify the agreement), for instance by posing as a third party.

INDEMNIFICATION AND DISPUTE RESOLUTION

- If you break this agreement, you may have to reimburse affected protocol members and may be subject to criminal prosecution.
- Either party may initiate a dispute for issues not resolved after 30 days. Disputes are resolved via binding arbitration, which will take place in Singapore under the administration of SIAC (Singapore International Arbitration Centre) unless otherwise specified by the agreement.
- If a dispute does arise, each side must pay half of the initial fees for the arbitrator and half of the regular expenses during the proceedings. All other costs, including attorney fees, will be paid by the loser after a judgment is reached.
- No member of the protocol can press claims of their own without the protocol's approval.

TAX, see Section 8.12 of the Agreement

COMPLIANCE WITH LAWS

- The protocol is not responsible for ensuring that, aside from the rescue itself, you are following the law both generally and with respect to the protocol.
- The protocol and its users will neither pursue nor assist any claims against you in connection with the rescue.

TERMS AND TERMINATION

- This agreement comes into effect immediately once adopted by protocol governance, and remains active until explicitly terminated.

MISCELLANEOUS PROVISIONS

- You can communicate with the protocol via the email listed in the agreement.
- The protocol can communicate with you via any address you use to make deposits to the ARA.
- You are responsible for any taxable events that occur as a result of the rescue. Generally, the safest and best thing to do is deposit funds *directly* to the ARA so that they never enter your direct possession.
- By participating, you waive your right to any class-action suits or trial by jury (because disputes are covered by arbitration).

EXHIBITS AND ADDENDA

- Exhibit A specifies certain defined terms used in the Agreement.
- Exhibit B outlines the recommended format for proposing adoption of the Agreement to a DAO.
- Exhibit C provides a form of consent for the Security Team to sign to adopt the Agreement.
- Exhibit D provides a form of procedures to be included in web applications and other user interfaces facilitating use of the Protocol to bind Users to the Agreement.
- Exhibit E provides recommended risk disclosures relating to adoption and use of the Agreement.
- Exhibit F provides an FAQ relating to the Agreement.

Things you must always check:

- List of eligible and ineligible exploits
- The Asset Recovery Address matches on all relevant communications and the on-chain registry
- There is not already a bug bounty program and responsible disclosure process in place that you can and should execute first
- You have NO OTHER PROFIT MOTIVE other than that of the reward. Anyone found to have an extraneous motive would not qualify for immunity

[Full summary including procedural recommendations found here](#)

BY PARTICIPATING IN THE PROGRAM, YOU WILL BE ENTERING INTO AND CONSENTING TO BE BOUND BY, AND ASSENTING TO THE TERMS AND CONDITIONS SET FORTH IN THE AGREEMENT, AND WILL BE DEEMED A PARTY TO THE AGREEMENT. PARTICIPATING IN THE PROGRAM INCLUDES, WITHOUT LIMITATION, TAKING ANY ACTION PURSUANT TO,

OR SEEKING TO RECEIVE ANY OF THE RIGHTS OR BENEFITS RELATED TO, THE PROGRAM, AS SET FORTH IN THE AGREEMENT.

NOTICE TO PARTICIPATING WHITEHAT, IF YOU DO NOT ABIDE BY, AND PERFORM ALL OF THE TERMS AND CONDITIONS OF THE AGREEMENT, OR IF ANY OF THE REPRESENTATIONS AND WARRANTIES SET FORTH IN THE AGREEMENT ARE INACCURATE AS APPLIED TO YOU, YOU MAY FAIL TO BE ELIGIBLE FOR OR ENTITLED TO ANY OR ALL RIGHTS OR BENEFITS UNDER THE AGREEMENT, INCLUDING ANY RIGHT TO RECEIVE OR RETAIN ANY BOUNTIES.

Please contact us at safeharbor@securityalliance.org for any questions or issues.

WHITEHAT SAFE HARBOR AGREEMENT

This **WHITEHAT SAFE HARBOR AGREEMENT (this “Agreement”)** sets forth the terms and conditions of the Program and is being entered into by, and is binding upon, each Protocol Community that adopts the Agreement and each Whitehat who conducts or attempts an Eligible Funds Rescue (collectively referred to as “*Parties*”). Certain capitalized terms used in this Agreement are defined on Exhibit A.

BACKGROUND INFORMATION

A. This Agreement has been prepared by the Security Alliance as part of an open source software implementation for decentralized technologies (i.e., on-chain protocols) within the blockchain/crypto ecosystem to incentivize and give comfort to Whitehats rescuing digital assets from active Exploits of a Protocol with respect to which this Agreement has been adopted by the relevant Protocol Community (each an “*Eligible Funds Rescue*” that mitigates an “*Urgent Blackhat Exploit*”, as defined below), and to provide a safe harbor for assets that are the subject of such an exploit.

B. Each Protocol Community adopting this Agreement for its corresponding Protocol seeks to encourage Whitehats to responsibly test, seek to penetrate, and otherwise take advantage of the Protocol, and, pursuant to the Program, potentially receive a Reward for conducting Eligible Funds Rescues. Only Whitehats who agree to the terms and conditions of this Agreement and conduct an Eligible Funds Rescue pursuant to and in accordance with the terms and conditions of this Agreement will be eligible to participate in the Program and potentially receive a Reward.

C. Each Whitehat adopting this Agreement seeks to test and exploit a Protocol with respect to which this Agreement has been adopted by the Protocol Community, for the purpose of completing an Eligible Funds Rescue within the bounds set out in this Agreement, and accordingly wishes to enter into this Agreement to participate in the Program and become eligible to potentially receive a Reward pursuant to the parameters set forth herein. Each Whitehat should ensure that such Whitehat has sufficient experience to participate in the Program, including because such Whitehat is an experienced software developer, security professional, software engineer, or an Entity that employs or engages experienced blockchain software engineers or security professionals (e.g., auditors) with expertise in the exploitation of blockchain systems and the mitigation of attendant risks.

Agreement

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties to this Agreement, intending to be legally bound, hereby agree as follows:

1 1. Eligible Protocols

1.1 Adoption of this Agreement by Protocol Communities.

- (a) A Protocol is eligible for Eligible Funds Rescues under this Agreement if this Agreement has been duly adopted by the Protocol Community associated with such Protocol in accordance with the Adoption Procedures, and such adoption has not been subsequently renounced, revoked, annulled, voided, or rescinded by the Protocol Community. It is recommended that

the DAO Adoption Procedures be accompanied by notices, information and disclosures based on those set forth on Exhibit B.

(b) This Agreement shall be:

- (i) binding upon and enforceable against any DAO with respect to any Protocol, by the DAO adopting this Agreement in accordance with the DAO Adoption Procedures;
- (ii) after adoption of this Agreement by the DAO Adoption Procedures, binding upon and enforceable against any Security Team with respect to any Protocol, by the Security Team adopting this Agreement in accordance with the Security Team Adoption Procedures; and
- (iii) after adoption of this Agreement by the DAO Adoption Procedures, binding upon and enforceable against any Users with respect to any Protocol, by the Users adopting this Agreement in accordance with the User Adoption Procedure.

(c) “**DAO Adoption Procedures**” means that this Agreement has been duly adopted and approved by or on behalf of a DAO by such DAO, by DAO Approval, or a person, group, entity, or other smart contract expressly and specifically authorized by DAO Approval to act for or on behalf of such DAO in such respect, having properly executed a call of the `adoptSafeHarbor` function of an instance of the official SEAL SafeHarborRegistry.sol (<https://github.com/security-alliance/safe-harbor/tree/main/registry-contracts>) that has been deployed to address `0x8f72fcf695523A6FC7DD97EafDd7A083c386b7b6` on a compatible blockchain system, with such call successfully setting the `AgreementDetailsV1` struct determining the terms of the Protocol Community’s adoption of this Agreement in accordance with the SafeHarborRegistry.sol code, including:

- (i) the `protocolName` (being a string specifying the name of the Protocol governed by such DAO, for which this Agreement is being adopted by such DAO);
- (ii) the `Chain[] chains`, being a struct specifying, for each `chain` on which an Eligible Funds Rescue from the Protocol is intended to be authorized:

(A) the `chainID` of such chain;

(B) the `assetRecoveryAddress` on such chain (which shall be the Asset Recovery Address with respect to the instance of the Protocol on such chain for Eligible Protocol Rescues pursuant to this Agreement); and

(C) the `Accounts [] scope` (being a struct specifying, for each blockchain account (which may be an ‘externally owned’ or ‘smart contract’ account) included in the Protocol on such `chain` for purposes of Eligible Funds Rescues of the Protocol on such `chain`;

- (1) the `accountAddress` of such account on such `chain`;
 - (2) the `ChildContractScope childContractScope` for such account, which specifies whether, with respect to the child contracts created by the `accountAddress`:
 - (w) none of such contracts are in scope for Eligible Funds Rescues (the `None` parameter);
 - (x) only such contracts as were created by such `accountAddress` prior to calling `adoptSafeHarbor` are in scope for Eligible Funds Rescues (the `ExistingOnly` parameter); and
 - (y) all such contracts, whether created by `accountAddress` before or after calling `adoptSafeHarbor`, are in scope for Eligible Funds Rescues (the `All` parameter); and
 - (z) only such contracts as are created by such `accountAddress` after the time `adoptSafeHarbor` is called are in scope for Eligible Funds Rescues (the `FutureOnly` parameter);
 - (3) optionally, the `signature` for such account, which may be used as additional evidence that such account has affirmatively accepted being subject this Agreement.
- (iii) the `Contact[] contactDetails` (being a struct specifying, for each individual or entity who should be contacted by Eligible Whitehats for notices to the Protocol Community pursuant to this Agreement, the `name` of such person within the Protocol Community and the `contact` details (e.g., email, phone, telegram handle, etc.) of such person for purposes of receiving notifications pursuant to this Agreement, including for purposes of receiving pre-rescue notifications pursuant to [Section 2.4\(c\)](#));
 - (iv) the `BountyTerms bountyTerms` (being a struct specifying the Bounty Percentage (the `bountyPercentage` string), the Bounty Cap (the `bountyCapUSD` integer), the Aggregate Bounty Cap (the `aggregateBountyCapUSD` integer, representing the maximum total aggregate dollar amount of Bounties payable to all Eligible Whitehats in connection with a single Exploit or series of related Exploits), whether or not the Bounty can be paid as a Retained Bounty (the `retainable` boolean); if `aggregateBountyCapUSD` is specified, retainable must be set to false to ensure accurate enforcement of the Aggregate Bounty Cap), the `IdentityRequirement identityRequirement` struct (specifying whether the Eligible Whitehat can be `Anonymous` or `Pseudonymous` or rather must confirm their legal name (`Named`))

and any KYC, sanctions, diligence or other verification that the Protocol Community will require be performed on the Eligible Whitehat in order to qualify for payment of the Bounty (the `diligenceRequirements` string);

- (v) the `agreementURI` (being the IPFS hash of the exact text of the official version of this Agreement as of the date of adoption).
- (d) In the event that a Protocol does not have a DAO, the Security Team may utilize the DAO Adoption Procedures to indicate adoption of this Agreement with respect to the Protocol, and, in such event, references in this Agreement to the DAO shall instead be treated as references to the Security Team.

1.2 Uncertain Legal Classification of DAOs; Enforceability.

- (e) Uncertain Legal Classification of DAOs. It is hereby acknowledged and agreed that the legal classification of participating DAOs may be uncertain. There may exist uncertainties as to whether a DAO is a continuous single legal person, the criteria and term of membership in a DAO for persons participating in DAO-related activities, the rules by which the DAO or any member of or participant in the DAO may become a party to or bound by any agreement, and the applicability of any such agreement to prior or future members of or participants in the DAO.
- (f) Enforceability. In light of the potential for the uncertain legal classification of DAOs to affect the enforceability of this Agreement against the DAO, any participants in or members of the DAO or the Protocol Community generally, the following non-exclusive order of preference concerning the Adoption Procedures and the subsequent enforceability of this Agreement is hereby acknowledged and agreed:
 - (i) If the DAO governing a Protocol is deemed to constitute a legal person and this Agreement is adopted through the DAO Adoption Procedures, then the DAO Adoption Procedures are intended to and shall be deemed to make this Agreement binding upon such legal person;
 - (ii) If the DAO governing a Protocol is deemed to be capable of binding the Protocol Community or Protocol Community Members to this Agreement through the DAO Adoption Procedures, then the DAO Adoption Procedures are intended to and shall be deemed to make this Agreement binding upon the Protocol Community and any and all Protocol Community Members, to the maximum extent permissible;
 - (iii) If the individual past, present, and/or future participants in or members of the DAO governing such Protocol may be bound to an agreement through the DAO Adoption Procedures, then the DAO Adoption Procedures are intended to and shall be deemed to

make this Agreement binding upon all such individual participants or members to the maximum extent permissible; or

- (iv) If the DAO is not deemed to be a legal person and it is not legally permitted to bind all individual past, present, and/or future participants in or members of the DAO hereto through the DAO Adoption Procedures, then, to the maximum extent permissible, this Agreement shall be deemed binding upon the individual Protocol Community Members, Users, or other persons who voted in favor of or otherwise expressly consented to, ratified, or affirmed this Agreement through the DAO Adoption Procedures, User Adoption Procedures, or otherwise.

1.3 Certain Defined Terms.

For purposes of this Agreement, the following capitalized terms have the meanings that are ascribed to them below:

- (a) ***“Adoption Procedures”*** means:
 - (i) the DAO Adoption Procedures;
 - (ii) the Security Team Adoption Procedures; and
 - (iii) the User Adoption Procedures.
- (b) ***“DAO”*** means any Entity or group or set of persons, whether or not incorporated, associated, or affiliated, that in-whole or in-part govern:
 - (i) a blockchain-based protocol; or
 - (ii) any funding, personnel or resources dedicated or reserved primarily for maintenance, development, marketing, operation, or improvement of any blockchain-based protocol,

provided, in each case, that such governance is achieved primarily through the voting of transferable votable Tokens (or non-transferable voting positions convertible from and into such Tokens).
- (c) ***“DAO Approval”*** means, with respect to a given DAO governing a Protocol and a given matter or action, that such matter or action has been validly approved in accordance with the specific governance process of the Protocol.
- (d) ***“Security Team”*** means, with respect to a given Protocol, any Entity, person, or group of persons (other than a DAO) having any privileges or powers with respect to the upgrading, parameterization, freezing, or upgrading of a Protocol or recovery of funds from an Exploit of a Protocol or vetoing or co-approval of proposals with the DAO governing such Protocol.
- (e) ***“Security Team Adoption Procedures”*** means that this Agreement has been duly adopted and approved on behalf of the Security Team by means of the execution and delivery of the Security Team (or one or more authorized representatives thereof) of a contract in

substantially the form attached hereto as Exhibit C and such contract has been published and is generally made available to the Protocol Community.

- (f) “**Users**” of a Protocol means all persons who have Tokens on deposit with, held by, or otherwise subject to the full or partial direct or indirect custody, control or influence of the Protocol.
- (g) “**User Adoption Procedures**” means the inclusion of provisions substantially in the form attached hereto as Exhibit D in the Terms of Service of at least a majority of the web applications specifically used to facilitate User interactions with the Protocol.
- (h) “**Protocol**” means the **accountAddress** and child contracts thereof set during the DAO Adoption Procedures, such accounts being the onchain systems for which the Protocol Community has adopted the Program and sought to make eligible the conduct of Eligible Funds Rescues by adopting this Agreement through the Adoption Procedures.
- (i) “**Protocol Community**” means, with respect to a given blockchain-based protocol at a given time, all of the Protocol Community Members as of such time.
- (j) “**Protocol Community Member**” means, with respect to a given blockchain-based protocol at a given time, each of:
 - (i) the DAO governing such protocol;
 - (ii) each User of such protocol; and
 - (iii) the Security Team for such protocol and each member of such Security Team.
- (k) “**Token**” means all tokens, cryptocurrencies, virtual assets, digital assets and other units of account or mediums of exchange that are transferable on a blockchain system.

2.2. COVERED Exploits & Rewards

2.1 Eligible Whitehats to be Compensated for Eligible Funds Rescues

If an Eligible Whitehat performs an Eligible Funds Rescue pursuant to and in accordance with this Agreement, then, as the sole compensation and reward for such performance, the Eligible Whitehat may be entitled to: (i) payment or retention of the applicable Bounty as set forth in Section 3; and (ii) the grant of a release of Claims as set forth in Section 6.2 (the consideration described in the preceding clauses ‘(i)’ and ‘(ii)’, collectively, the “**Reward**”).

2.2 Limited Scope

This Agreement and the Reward granted hereunder are intended solely to provide compensation to Eligible Whitehats who complete Eligible Funds Rescues of Tokens from an Urgent Blackhat Exploit (as defined below).

All other pending, threatened, or possible Exploits; security vulnerabilities; or other facts and circumstances relating to a Protocol are not addressed by this Agreement and may be addressed, for example, through an ordinary security bounty program, or other rules, procedures, and agreements applicable to such Protocol.

2.3 Certain Defined Terms

- (a) Exploit. An “**Exploit**” means an attack, hack, or exploit against all or any part of a Protocol.
- (b) Eligible Whitehat. A Person (other than the owner/operator of a Generalized Arbitrage Bot) is an “**Eligible Whitehat**” with respect to a particular Exploit if and only if such person:
 - (i) has read, understood, and agreed to be bound by this Agreement with respect to such Exploit;
 - (ii) the representations and warranties in Section 5 are accurate and complete as to such person in connection with and at all times relevant to such Exploit;
 - (iii) such person has not breached, contravened or violated any provision of this Agreement or any applicable or otherwise relevant law, legal order or any legally binding agreement in connection or at any time relevant to such Exploit;
 - (iv) such person has fully complied with the requirements of Section 2.4 with respect to such Exploit; and,
 - (v) the Reward comprises such person’s sole direct and indirect compensation, reward, and benefit in connection with the Exploit.
- (c) Eligible Funds Rescues. An “**Eligible Funds Rescue**” is an Exploit and related actions or transactions that, taken together:
 - (i) intercept, interrupt, block, interfere with, impede, disrupt, prevent, or mitigate the adverse effects of, an Urgent Blackhat Exploit;
 - (ii) result in the complete transfer of all Returnable Assets (or the transfer of all Returnable Assets, *minus* the applicable Bounty) to the Asset Recovery Address as promptly as reasonably practicable during or after such Exploit (except that, in the case of such an Exploit performed by a Generalized Arbitrage Bot, such transfer may be effected as promptly as reasonably practicable after the owner/operator of the Generalized Arbitrage Bot discovers that the Generalized Arbitrage Bot has executed such Exploit, but in no event more than 72 hours after such Exploit);
 - (iii) have been performed in good faith solely for the purposes described in the preceding clauses ‘(i)’ and ‘(ii)’ and to earn the Reward (except that in the case of an Exploit automatically executed by a Generalized Arbitrage Bot, there need be no specific intent of the kind described in the preceding clause ‘(i)’);

- (iv) are not conducted in a negligent, reckless, or fraudulent manner and do not constitute an intentional, knowing, reckless, or negligent breach of any applicable or otherwise relevant law, legal order, or any legally binding agreement; and
- (v) otherwise comply with and satisfy all applicable terms and conditions of this Agreement.
- (d) Generalized Arbitrage Bot. A “**Generalized Arbitrage Bot**” is software that autonomously monitors and analyzes substantially all transaction requests submitted to a blockchain network’s mempool and seeks to automatically arbitrage or gain execution priority over third-party transactions for financial profit.
- (e) Urgent Blackhat Exploits. “**Urgent Blackhat Exploit**” means an Exploit that, based on publicly available or otherwise verifiable information, would reasonably be considered to:
 - (i) (A) have already been initiated against a Protocol and remain an active threat; or (B) be highly likely to be imminently initiated against a Protocol; and
 - (ii) constitutes a reckless, malicious, illegal, unlawful, or otherwise harmful Exploit against a Protocol that is highly likely to imminently result in the loss, theft, misappropriation, freezing or other adverse impact on any Tokens directly or indirectly controlled by, deposited into, held by, or custodied with the Protocol, and for which the Whitehat is confident that a normal course bug bounty referral will not be sufficient to protect the funds.

2.4 Required Procedures For Attempting Eligible Funds Rescues.

- (a) Prospective Whitehats vs Retrospective Whitehats. Each person attempting or undertaking an Eligible Funds Rescue, seeking a Reward, or seeking the benefit of the consent to Exploits set forth in Section 2.4(b) is referred to herein as a “**Whitehat**”. A Whitehat that is the owner/operator of a Generalized Arbitrage Bot who, upon discovering that an Exploit against a Protocol has been effected by such Generalized Arbitrage Bot, attempts or undertakes an Eligible Funds Rescue, is referred to herein as a “**Retrospective Whitehat**” and all other Whitehats are referred to herein as “**Prospective Whitehats**”.
- (b) Consent to Exploit by Prospective Whitehats. In the event that an Urgent Blackhat Exploit is highly likely to be imminently initiated or in process with respect to a Protocol and a Prospective Whitehat who satisfies the eligibility conditions set forth in clauses ‘(i)’ through ‘(iii)’ of Section 2.3(b) could reasonably be expected to complete an Eligible Funds Rescue with respect to such Urgent Blackhat Exploit, then, for so long as the Urgent Blackhat Exploit remains imminent or in process and such Prospective Whitehat otherwise complies with this Agreement, the Prospective Whitehat is hereby granted the consent of the Protocol Community to use best efforts to attempt the Eligible Funds Rescue with respect to the smart contracts included in the assets [deemed in scope by the Protocol Community], including by

seeking to satisfy (or continuing to satisfy, as applicable) the eligibility conditions set forth in clauses ‘(ii)’ through ‘(v)’ of Section 2.3(b) so as to become an Eligible Whitehat and by performing a permitted type of Exploit (as contemplated by Section 2.3(c)) against the Protocol to the extent necessary to intercept, interrupt, block, interfere with, impede, disrupt, prevent, or mitigate the adverse effects of, such Urgent Blackhat Exploit.

(c) Notification of Attempted Eligible Funds Rescue.

- (i) The Whitehat shall use commercially reasonable efforts to notify the Protocol Community that the Whitehat is attempting an Eligible Funds Rescue as soon as reasonably practicable in accordance with Section 9.6.
- (ii) For Prospective Whitehats, it is strongly recommended, although not required, to deliver such notification prior to initiating an Exploit against the Protocol if doing so would not adversely affect the likelihood of achieving an Eligible Funds Rescue. For Retrospective Whitehats, it is strongly recommended that the Whitehat deliver such notification immediately after discovering that the Generalized Arbitrage Bot owned or operated by such Whitehat has executed an Exploit against the Protocol.

(d) Transfer of Assets to Asset Recovery Address.

- (i) The Whitehat shall at all times use best efforts to secure, and preserve the value of, all Exploited Assets.
- (ii) Upon removing, appropriating, diverting, or otherwise obtaining custody or control over any Exploited Assets, the Whitehat must use best efforts to transfer them to the Asset Recovery Address as promptly as reasonably practicable, as follows:
 - (A) If the Adopting Procedures for the relevant Protocol expressly allow for the Whitehat to deduct and retain the Bounty from the Exploited Assets, then the Whitehat shall transfer all Returnable Assets *minus* the applicable Bounty, into the Asset Recovery Address as promptly as reasonably practicable.
 - (B) If the Adopting Procedures for the relevant Protocol do not expressly allow for the Whitehat to deduct and retain the Bounty from the Exploited Assets, then the Whitehat shall transfer all Returnable Assets into the Asset Recovery Address as promptly as reasonably practicable.

An Exploit with respect to which the Returnable Assets have not been so transferred into the Asset Recovery Address in accordance with the preceding clause ‘(A)’ or clause ‘(B)’, as applicable, shall not constitute an Eligible Funds Rescue and the Whitehat shall not be entitled to any Reward with respect thereto. In either case, if a Whitehat is unable to transfer the Returnable Assets into the Asset Recovery Address within six hours of obtaining custody or control over them, then the Whitehat must notify the Protocol Community, in accordance with Section 9.6, of their continued intention to transfer the

Returnable Assets into the Asset Recovery Address and the reasons for their inability to transfer those assets.

- (iii) “**Exploited Assets**” means, with respect to a given Urgent Blackhat Exploit, all Tokens that, directly or indirectly in connection with such Exploit, have been in whole or in part removed, appropriated, diverted, or otherwise obtained by or on behalf of a Whitehat from the Protocol.
- (iv) “**Asset Recovery Address**” means the blockchain network address to which Eligible Whitehat Hackers shall deposit the Returnable Assets—i.e., the address selected as the `assetRecoveryAddress` parameter during the DAO Adoption Procedures.
- (v) “**Returnable Assets**” means, with respect to a given Urgent Blackhat Exploit, all of the Exploited Assets recovered by a Whitehat, *minus* any Exploited Assets utilized by the Whitehat in good faith, arms-length transactions to pay transaction fees or costs necessary to perform the Exploit and return Exploited Assets to the Asset Recovery Address (including any value or Tokens lost as a result of “extractable value” or other arbitrage by validators or other third parties), provided that in each case the Whitehat used best efforts to minimize such fees and costs.

3 Eligibility, Release and Bounty

3.1 Eligibility Conditions

- (a) Conditions Precedent. Each clause of the terms “Eligible Whitehat” and “Eligible Funds Rescue,” and the fulfillment of each requirement set forth in the `IdentityRequirement` `identityRequirement` struct and `diligenceRequirements` string of the `BountyTerms` `bountyTerms` struct set by the DAO Adoption Procedures, shall be conditions precedent to any person’s entitlement to receive a Reward. Such conditions precedent are in furtherance and not in limitation of the other terms and conditions of this Agreement. In the event that a Whitehat receives or retains a Bounty (or any portion thereof) at a time when any of the aforementioned conditions precedent were not satisfied, the Bounty shall be deemed forfeit and the Whitehat shall, upon demand by the Protocol Community or any Protocol Community Member, immediately transfer the full amount of any Retained Bounty directly to the Asset Recovery Address.
- (b) Relationship of Protocol Community to Whitehat. Under no circumstances do the Protocol Community or any Protocol Community Member seek through this Agreement to facilitate, encourage, or condone any conduct by Whitehat that violates any Legal Requirement under any applicable jurisdiction or any fraudulent, misleading, manipulative, reckless, or negligent conduct by Whitehat towards any Party or non-party to this Agreement. The Protocol Community disclaims any liability or direct or consequential damages caused by Whitehat by participating in the Program, and make no representations or warranties to Whitehat that

participation in the Program under the terms of this Agreement will protect Whitehat from liability except as otherwise specified in Section 6.2 below.

3.2 Bounty

- (a) Bounty. **“Bounty”** means, with respect to a particular Urgent Blackhat Exploit and the resulting Eligible Funds Rescue(s) completed by an Eligible Whitehat, Tokens equal in US Dollar value to *lesser of*: (i) the **bountyPercentage** (specified during the DAO Adoption Procedures) of the US Dollar value, based on the timestamp of the block that was proposed in the Protocol immediately preceding the Eligible Funds Rescue, of Returnable Assets recovered by each Eligible Whitehat and transferred to the Asset Recovery Address from such Eligible Whitehat’s originating blockchain address(es); or (ii) the **bountyCapUSD** (specified during the DAO Adoption Procedures); *provided, however*, that notwithstanding the foregoing definition of “Bounty” or any other provision of this Agreement the total aggregate amount of all Bounties payable to all Eligible Whitehats in connection with a particular Exploit or series of related Exploits shall not exceed the **aggregateBountyCapUSD** (as specified during the DAO Adoption Procedures) (the **“Aggregate Bounty Cap”**). If the total U.S. dollar value of Bounties payable to all Eligible Whitehats in connection with a particular Exploit or series of related Exploits would otherwise exceed the **aggregateBountyCapUSD**, then such Bounties shall be automatically deemed reduced on a pro rata basis such that the total aggregate U.S. dollar value of all such Bounties equals the **aggregateBountyCapUSD**.
- (b) Payment of Bounty. Following the completion of an Eligible Funds Rescue and the determination that the Whitehat is eligible for a Reward pursuant to the terms of this Agreement:
 - (i) In the event that the Whitehat has returned all of the Returnable Assets, the Protocol Community will pay the Bounty to the Whitehat, subject to the terms of this Agreement. Payment of the Bounty is to be made to the Whitehat’s address as nominated at the time of delivery of the Returnable Assets to the Asset Recovery Address. In the event that the Protocol Community fails to transfer the Bounty to the Whitehat within a reasonable time (and in no event more than 15 calendar days after the date that the first or only Returnable Assets are sent to the Asset Recovery Address), or in the event that the Whitehat and Protocol Community are unable to agree upon the amount of the Bounty, the Reward Dispute Procedures, as set forth in Section 3.3, shall apply. The Protocol Community may, in its reasonable discretion, require that a Whitehat provide backup withholding documentation (such as Form W-9 or W-8 (series) for Protocol Communities subject to income taxation in the United States), and, if not provided in a reasonable amount of time, deduct the required amounts of backup withholding from any such Bounty payment to a Whitehat.

- (ii) In the event that (A) the `retainable` boolean was set to TRUE in the DAO Adoption Procedures; and (B) the Whitehat has retained the Bounty, and sent all Returnable Assets to the Asset Recovery Address less the amount retained by the Whitehat as the Bounty (a “**Retained Bounty**”), the Whitehat shall verify in writing to the Protocol Community the address at which the Retained Bounty is located and not move the Retained Bounty from this address. The Protocol Community shall, within a reasonable time and in no event more than 15 calendar days, send written verification to the Whitehat as to whether the Protocol Community disputes the amount of the Retained Bounty. In the event no notice is sent to the Whitehat within the timeframe specified in the preceding sentence, the Retained Bounty amount shall be presumed acceptable to the Protocol Community. In the event that the Protocol Community disputes the amount of the Retained Bounty, the Reward Dispute Procedures, as set forth in Section 3.4, shall apply. If there is an Aggregate Bounty Cap (as determined during the DAO Adoption Procedures and referred to in Section 3.2(a) above), then there must be no Retained Bounty (as determined during the DAO Adoption Procedures). This ensures the Protocol Community can accurately enforce the Aggregate Bounty Cap and allocate payouts on a pro rata basis.

3.3 Reward Dispute Procedures

- (a) Reward Dispute Procedures. In the event that a dispute between the Protocol Community exists as to: (x) the amount of a Bounty, (y) whether the Whitehat is entitled to a Reward; or (z) whether the Bounty is subject to offset pursuant to Section 7.1(a) below (each, a “**Reward Dispute**”), the Parties shall identify the amount of the Bounty and all other aspects of the Reward which are disputed (the “**Disputed Amount**”) and the following procedures shall apply.
 - (i) If the Reward Dispute relates to the value of the tokens comprising the Bounty only (i.e., if the Protocol Community and Whitehat agree that the Whitehat is entitled to a Reward, but cannot agree on the value of the Bounty), the Party in possession of the Disputed Amount shall transfer the Disputed Amount into an escrow account that requires the signature of the Whitehat and Protocol Community to be released. Each Party shall, within 30 calendar days, appoint an appraiser or other valuation expert to render an opinion as to the proper amount of the Bounty (an “**Appraisal**”). In the event that the higher of the Appraisals is no greater than 130% of the lower Appraisal, the Bounty shall be the average of the two Appraisals. In the event that the higher of the Appraisals is greater than 130% of the lower Appraisal, the appraisers shall appoint a neutral third-party appraiser, whose Appraisal shall control the amount and allocation of the Bounty. Upon the conclusion of this appraisal process, the Parties shall release the

escrowed Bounty amount(s) to whichever Party is entitled to all or a portion of the Disputed Amount.

- (ii) If the Reward Dispute relates to the entitlement of the Whitehat to a Reward, a Claim by an Indemnitee gives rise to a Disputed Amount, or if the dispute relates to the amount of Returnable Assets owed to the Protocol Community, the Arbitration provisions of Section 7.1(b) shall apply.

4 Certain Covenants and Agreements of Whitehat

- 4.1 Legal Compliance.** Whitehat shall at all times ensure that their actions are in compliance with all applicable Legal Requirements. Whitehat acknowledges that Protocol Community will not, and has no legal obligation to, monitor the legal compliance of Whitehat in relation to Whitehat seeking to perform an Eligible Funds Rescue.
- 4.2 Non-Exclusivity.** Whitehat acknowledges and agrees that there shall be no relationship of exclusivity between Whitehat and Protocol Community; Protocol Community shall be fully entitled to permit other Persons (who may be competitors of Whitehat) to participate in the Program; and neither the Protocol Community nor any Protocol Community Member is making any covenant, commitment, agreement or undertaking to keep Whitehat informed regarding the progress or involvement of other Persons participating in the Program or to treat Whitehat equally with such other Persons.
- 4.3 No Partnership, Agency or Similar Relationship.** For the purposes of this Agreement, Whitehat acknowledges and agrees that Whitehat shall not be deemed to be part of any partnership, joint venture, unincorporated association, or other Entity with Protocol, any Representative of the Protocol Community, or any Protocol Community Member; further, Whitehat shall not be deemed an employee, independent contractor, or other Representative of the Protocol Community or any Protocol Community Member. Whitehat also represents that it will not hold itself out as having, represent that it has, or induce or knowingly permit any Person to believe that it is a Representative of the Protocol Community or any other Protocol Community Member arising out of or in connection with this Agreement, the Program, or the performance or attempt of any Eligible Funds Rescue.
- 4.4 No Guarantees or Assurances of Rewards.** Other than as expressly provided for in this Agreement, Protocol Community shall not be deemed to be directly or indirectly providing any express or implied guarantee or assurance that Whitehat will receive any Rewards. Protocol Community may, at any time, in its sole discretion, cancel and terminate such Protocol Community's participation in the Program; *provided, however*, that the Protocol Community shall not be permitted to terminate the Program with respect to any completed or in-progress Eligible Funds Rescue. Whitehat hereby assumes all risks that they do not qualify for any Rewards, regardless of the level of time or effort or cost expended by Whitehat in pursuit of the Rewards.

5 Representations and Warranties of Whitehat

Whitehat hereby represents and warrants to and for the benefit of Protocol Community and Protocol Community Members, their Affiliates and their respective Representatives (it being acknowledged and agreed by Whitehat that Protocol Community is relying on, and would not have entered into this Agreement without the representations and warranties set out in this Section 5), as follows:

5.1 Authority and Due Execution

- (a) Authority. Whitehat has all requisite capacity, power and authority to enter into, and perform Whitehat's obligations under, this Agreement and to fully participate in the Program. The execution, delivery and performance of, and the performance of Whitehat's obligations under this Agreement and Whitehat's full participation in the Program have been duly authorized by all necessary action on the part of Whitehat and, if Whitehat is an Entity, its board of directors or comparable authority(ies), and no other proceedings on the part of Whitehat are necessary to authorize the execution, delivery or performance of this Agreement by Whitehat.
- (b) Due Execution. This Agreement has been duly accepted by Whitehat and constitutes the legal, valid and binding obligation of Whitehat, enforceable against Whitehat in accordance with its terms.

5.2 Money Laundering and Sanctions. To the best of Whitehat's knowledge, any crypto-assets or funds that are or will be obtained, leveraged, recovered, exploited, or otherwise used by Whitehat in any Eligible Funds Rescue were not and are not directly or indirectly derived from any activities that contravene any law, rule, regulation or order (including anti-money laundering laws and regulations) applicable to the Whitehat. None of: (a) Whitehat; (b) any Affiliate of Whitehat; (c) any person having a beneficial interest in the Whitehat (if an Entity); or (d) any person for whom the Whitehat is acting as agent or nominee in connection with this Agreement is: (i) a country, territory, Entity or individual named on an OFAC list as provided at <http://www.treas.gov/ofac>, or a person or Entity subject to sanctions or prohibitions under OFAC or any other national or international sanctions regime, regardless of whether or not they appear on the OFAC list; or (ii) a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure.

5.3 Non-Contravention. The execution and delivery of this Agreement does not, and the performance of Whitehat's obligations under this Agreement and Whitehat's full participation in the Program will not: (a) if Whitehat is an Entity, conflict with or violate any of the charter documents of Whitehat or any resolution adopted by its equity holders or other Persons having governance authority over the Whitehat Entity; (b) contravene, conflict with, or violate any applicable Legal Requirement to which Whitehat, or any of the assets owned or used by Whitehat, is subject; or (c) result in any breach of or constitute a default (or an event that with notice or lapse of time or both

would become a default) under any material contract or agreement of Whitehat, permit held by Whitehat or Legal Requirement applicable to Whitehat.

5.4 Whitehat's Independent Investigation and Non-Reliance. Whitehat is sophisticated, experienced, and knowledgeable in the business of software exploits and blockchain exploits. Whitehat acknowledges and agrees that it is acting independently of Protocol Community in connection with this Agreement and the Program, and that the Protocol Community is not engaged in any exploit activities and has not evaluated, and makes no representation or warranty, express or implied, regarding, any benefits or risks of or necessary or desirable practices regarding any actions surrounding any attempt at an Eligible Funds Rescue. Additionally, Whitehat has conducted an independent investigation of the Protocol, the Program, and the matters contemplated by this Agreement, has formed its own independent judgment regarding the benefits and risks of and necessary and desirable practices regarding the foregoing, and, in making its determination to participate in the Program, Whitehat has relied solely on the results of such investigation and such independent judgment. Without limiting the generality of the foregoing, Whitehat understands, acknowledges and agrees that the Legal Requirements pertaining to blockchain technologies and Tokens generally, and the Protocol in particular, are uncertain, and Whitehat has conducted an independent investigation of such potentially applicable Legal Requirements and the resulting risks and uncertainties. Whitehat hereby irrevocably disclaims and disavows reliance upon any statements or representations made by or on behalf of, or information made available by, the Protocol Community or any Protocol Community Members, in determining to enter into this Agreement, or participate in the Program.

5.5 Litigation. There is no Legal Proceeding pending or threatened: (a) that involves Whitehat or any Representatives or Affiliates of Whitehat; and (b) related to or arising out of Whitehat's activities in connection with exploits of software or blockchain technologies or any other Token trading or blockchain technology related activities.

5.6 Intellectual Property and Related Matters. Whitehat is the sole and exclusive owner of all right, title and interest in and to all Intellectual Property Rights to all Technology incorporated into or otherwise used, held for use or practiced in connection with (or planned by Whitehat to be incorporated into or otherwise used, held for use or practiced during the course of the Program in connection with) the Program other than any Intellectual Property Rights that are validly licensed (or provided on a hosted basis) to Whitehat pursuant to valid and binding Intellectual Property Licenses granted to Whitehat.

5.7 Compliance; Orders

- (a) Compliance. Whitehat has complied with, and has not violated, any applicable Legal Requirement relating to any blockchain technologies, cybersecurity-related activities, or Token trading activities. No investigation or review by any Governmental Entity is pending or, to Whitehat's knowledge, has been threatened against or with respect to Whitehat.

- (b) Orders. To the Whitehat's knowledge, there is no legal order, decree, or other directive to which Whitehat or any Representative of Whitehat is subject that prohibits Whitehat or such Representative from engaging in or continuing any conduct, activity or practice relating to Whitehat's participation in the Program.

5.8 Full Disclosure. This Section 5 does not: (a) contain any representation, warranty, statement or information that is false or misleading with respect to any material fact; or (b) omit to state any material fact necessary in order to make the representations, warranties and information contained in this Section 5 (in the light of the circumstances under which such representations, warranties, statements and information were or will be made or provided) not false or misleading.

6 Releases

6.1 Mutual Release Among Protocol Community and Protocol Community Members.

- (a) Release. The Protocol Community collectively and each Protocol Community Member individually, hereby, to the extent permitted at law, irrevocably, unconditionally, and completely exculpates, releases, acquits and forever discharges the Protocol Community and each Protocol Community Member from, and hereby irrevocably, unconditionally, and completely waives and relinquishes, every Claim, that any Protocol Community or Protocol Community Member may have had in the past, may now have, or may have in the future against the Protocol Community or any Protocol Community Member, relating to or arising out of this Agreement or any Eligible Funds Rescue attempted or effected in connection herewith or any of the other matters contemplated hereby.
- (b) No-Litigation. The Protocol Community and each Protocol Community Member hereby agree not to assert or attempt to assert against the Protocol Community or any Protocol Community Member any Claim described under the preceding clause '(a)' of this Section 6.1.
- (c) Unknown Claims.
 - (i) If the Protocol Community or any Protocol Community Member may have any rights under Section 1542 of the Civil Code of the State of California, each such person hereby: (A) represents, warrants and acknowledges that such person (1) has been fully advised by such person's attorney of the contents of Section 1542 of the Civil Code of the State of California and (2) understands the implications thereof; and (B) hereby expressly waives the benefits thereof and any rights that they may have thereunder. Section 1542 of the Civil Code of the State of California provides as follows:

“A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE

MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR.”

- (ii) The Protocol Community and each Protocol Community Member hereby waives the benefits of, and any rights that any of them may have under, any statute, common law, or other Legal Requirement regarding the release of unknown claims in any jurisdiction.

6.2 Release of Whitehat Liability to Protocol Community

- (a) Release by Protocol Community. The Protocol Community and each Protocol Community Member, hereby, to the extent permitted at law, irrevocably, unconditionally, and completely exculpates, releases, acquits and forever discharges Whitehat from, and hereby irrevocably, unconditionally, and completely waives and relinquishes, every Claim, that any Protocol Community or Protocol Community Member may have had in the past, may now have, or may have in the future against Whitehat, relating to or arising out of each Eligible Funds Rescue successfully executed by or with the assistance of the Whitehat, including any Claim based on a theory of quantum meruit, promissory estoppel, or other equitable doctrine and any Claim contrary to any of the acknowledgements and assumptions of risk set forth in this Agreement; *provided, however*, that Whitehat shall not be released from any breach or non-compliance with the terms and conditions of this Agreement and provided further that this release does not apply to any indemnity owed by the Whitehat under Section 7.1(a).
- (b) No-Litigation. The Protocol Community and each Protocol Community Member hereby agree not to assert or attempt to assert against the Whitehat any Claim from which such Whitehat has been released under Section 6.2.
- (c) Unknown Claims.
 - (i) If the Protocol Community or any Protocol Community Member may have any rights under Section 1542 of the Civil Code of the State of California, each such person hereby: (A) represents, warrants and acknowledges that such person (1) has been fully advised by such person’s attorney of the contents of Section 1542 of the Civil Code of the State of California and (2) understands the implications thereof; and (B) hereby expressly waives the benefits thereof and any rights that they may have thereunder. Section 1542 of the Civil Code of the State of California provides as follows:

“A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR.”

- (ii) The Protocol Community and each Protocol Community Member hereby waives the benefits of, and any rights that any of them may have under, any statute, common law or other Legal Requirement regarding the release of unknown claims in any jurisdiction.

6.3 Release by Whitehat

- (a) Definitions. For purposes of this Section 6.3:
 - (i) “**Protocol Community Persons**” includes the Protocol Community, the Protocol Community Members, the Protocol Community’s Affiliates and the Protocol Community and Protocol Community’s Affiliates’ respective successors and past, present and future assigns and Representatives (hereafter); and
 - (ii) “**Whitehat Persons**” includes Whitehat, acting on Whitehat’s own behalf and on behalf of Whitehat’s Representatives and Affiliates.
- (b) Release. Whitehat (on Whitehat’s own behalf and on behalf of Whitehat Persons) hereby irrevocably, unconditionally, and completely releases, acquits, and forever discharges each of the Protocol Community Persons from, and hereby irrevocably, unconditionally, and completely waives and relinquishes, each and every Claim, that any Whitehat Person may have had in the past, may now have or may have in the future against any of the Protocol Community Persons, directly or indirectly relating to or directly or indirectly arising out of any event, matter, cause, thing, act, omission or conduct occurring, existing, or arising in connection with Whitehat’s or any other Whitehat Person’s participation in or involvement with the Program or execution or performance of this Agreement, including any Claim based on a theory of quantum meruit, promissory estoppel, or other equitable doctrine and any Claim contrary to any of the acknowledgements and assumptions of risk set forth in this Agreement; *provided, however*, that Whitehat is not releasing any rights expressly provided to Whitehat under this Agreement.
- (c) Unknown Claims.
 - (i) If Whitehat or any or other Whitehat Person may have any rights under Section 1542 of the Civil Code of the State of California, Whitehat hereby (on Whitehat’s own behalf and on behalf of the other Whitehat Persons): (A) represents, warrants, and acknowledges that Whitehat and such other Whitehat Persons (1) have been fully advised by their respective attorneys of the contents of Section 1542 of the Civil Code of the State of California and (2) understand the implications thereof; and (B) hereby expressly waive the benefits thereof and any rights that they may have thereunder. Section 1542 of the Civil Code of the State of California provides as follows:

“A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH IF KNOWN BY HIM OR HER MUST HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR.”

- (ii) Whitehat (on Whitehat’s own behalf and on behalf of the other Whitehat Persons) hereby waives the benefits of, and any rights that any of them may have under, any statute, common law, or other Legal Requirement regarding the release of unknown claims in any jurisdiction.
- (d) Necessary Actions. Whitehat represents and warrants that Whitehat has taken all actions necessary or appropriate to give full effect to the release given by Whitehat (on such Whitehat’s own behalf and on behalf of the other Whitehat Persons) in this Section.
- (e) Further Assurances. Without limiting the generality of Section 9.4, Whitehat agrees that Whitehat shall execute and deliver (and ensure that the other Whitehat Persons execute and deliver) to Protocol Community and the other Protocol Community Persons such instruments and other documents, and shall take (and ensure the other Whitehat Persons take) such other actions, as Protocol Community Persons may request in good faith for the purpose of carrying out or evidencing the release and related matters set forth in this Section. Without limiting the generality of the foregoing, Whitehat agrees that Whitehat will not assert or attempt to assert, and will ensure that none of the other Whitehat Persons will assert or attempt to assert, any Claim of the type released under Section 6.3(b) against any Protocol Community Person at any time after the execution and delivery of this Agreement.

7 Indemnification and Arbitrable Disputes

7.1 Indemnification

- (a) Indemnity. Whitehat shall hold harmless and indemnify Protocol Community, Protocol Community Members, their Affiliates, and their respective Representatives (collectively, the “*Indemnitees*”) from and against any Damages that are directly or indirectly suffered or incurred at any time following the Eligible Funds Rescue by any of the Indemnitees or to which any of the Indemnitees may otherwise directly or indirectly become subject at any time and which arise directly or indirectly from or as a result of, or are directly or indirectly connected with: (i) any material misrepresentation, inaccuracy, or omission in connection with any of the representations and warranties made by Whitehat; or (ii) any material breach or non-performance of the Agreement by Whitehat; provided that, the aggregate maximum amount of payment owed by the Whitehat under this Section 7.1(a) shall be limited to the amount of the Bounty due and actually received by the Whitehat hereunder. In the event that

no payment has been made to the Whitehat, the Whitehat's indemnity obligation shall reduce the amount of the Bounty otherwise owed to the Whitehat.

(b) Arbitrable Disputes.

- (i) In the event that the Indemnatee and Whitehat do not settle a claim for indemnification or any other action, suit, or other legal proceeding relating to this Agreement or the enforcement of any provision of this Agreement within 30 days after the date on which notice of such claim is delivered by one party (or Indemnatee) to the other, then such claim shall be deemed to be the subject of a dispute (an "**Arbitrable Dispute**").
- (ii) Each Arbitrable Dispute shall be settled by binding arbitration. Notwithstanding the preceding sentence, nothing in this Section 7 shall prevent the Indemnatee from seeking preliminary injunctive relief from a court of competent jurisdiction pending settlement of any Arbitrable Dispute.
- (iii) Except as herein specifically stated, any Arbitrable Dispute shall be resolved by arbitration in Singapore under the administration of the Singapore International Arbitration Centre ("**SIAC**") in accordance with the Arbitration Rules of the Singapore International Arbitration Centre (the "**SIAC Rules**") then in effect. However, in all events, the provisions contained in this Agreement shall govern over any conflicting rules which may now or hereafter be contained in the SIAC Rules. Any judgment upon the award rendered through arbitration shall be entered in any court having jurisdiction over the subject matter thereof and over the Person against whom the award rendered is to be enforced. Decisions rendered through arbitration shall have the authority to grant any equitable and legal remedies that would be available if any judicial proceeding was instituted to resolve an Arbitrable Dispute. A final decision rendered through arbitration may be submitted for entry to a court of competent jurisdiction. The existence and events and circumstances and outcome of such arbitration shall be treated as confidential and not disclosed or made public by the parties; *provided, however*, that (A) each party may discuss the arbitration on a confidential basis with their respective professional advisors, attorneys, directors, officers, members, and Affiliates; and (B) each party may disclose information solely to the extent necessary to enforce the results of the arbitration, provided that prior to any such disclosure such party uses (and affords the other parties an opportunity to use) commercially reasonable efforts to seek the confidential treatment of such information (e.g., by seeking a protective order).
- (iv) Any such arbitration will be conducted in English before a panel of three arbitrators who will be compensated for their services at a rate to be determined by the parties or by SIAC, but based upon reasonable hourly or daily consulting rates for each arbitrator in the event the parties are not able to agree upon his or her rate of compensation.

- (v) The members of the panel of arbitrators shall be mutually agreed upon by the parties. In the event the parties are unable to agree within 20 days following submission of the dispute to SIAC by one of the parties, SIAC will have the authority to select panel members from a list of arbitrators who satisfy the criteria set forth in clause ‘(vi)’ below.
- (vi) Each arbitrator must not have any past or present family, business or other relationship with the parties or any relevant Indemnatee, unless, following full disclosure of all such relationships, the parties and any relevant Indemnatee agree in writing to waive such requirement with respect to each arbitrator in connection with such dispute. In addition, unless otherwise agreed by the parties and any relevant Indemnatee in writing, an arbitrator in any dispute related to an Arbitrable Dispute shall have at least 15 years’ experience in the negotiation of complex corporate transactions; *provided, however*, that if SIAC is not able to provide an arbitrator for such arbitration with the requisite experience set forth in this clause ‘(vi)’, such arbitrator shall be a retired Article III Federal District Court judge of the United States with prior experience as an arbitrator.
- (vii) The parties will each pay 50% of the initial compensation to be paid to the arbitrators in any such arbitration and 50% of the costs of transcripts and other normal and regular expenses of the arbitration proceedings; *provided, however*, that: (A) the prevailing party in any arbitration will be entitled to an award of attorneys’ fees and costs; and (B) all costs of arbitration, other than those provided for above, will be paid by the losing party, and the arbitrator will be authorized to determine the identity of the prevailing party and the losing party. The losing party shall be determined solely by the arbitrator.
- (viii) The arbitrators chosen in accordance with these provisions will not have the power to alter, amend or otherwise affect the terms of these arbitration provisions or any other provisions contained in this Agreement.
- (ix) Any ruling or decision of the arbitrators may be enforced in any court of competent jurisdiction.

6.2. Exercise of Indemnification Remedies Other Than by Protocol Community. No Indemnatee (other than Protocol Community) shall be permitted to assert any claim to be held harmless, indemnified, compensated or reimbursed or to exercise any other remedy under this Agreement unless Protocol Community shall have consented to the assertion of such claim or the exercise of such other remedy (it being understood and agreed that no such consent by Protocol Community shall otherwise modify or operate as a waiver of the rights and obligations of any party to this Agreement). Protocol Community shall be entitled to act as agent for any Indemnatee in connection with any claim to be held harmless, indemnified, compensated or reimbursed or other remedy sought, asserted or exercised, or sought to be asserted or exercised.

8 7. Term and Termination

The applicability of the Program and the term of this Agreement for a given Protocol Community commence from the date when the Protocol Community adopts and ratifies this Agreement through the Adoption Procedures, and terminates upon the Protocol passing a proposal which terminates the Protocol Community's participation in the Program or adoption of this Agreement; *provided, however*, that no such termination shall affect terms that by their nature are intended to survive a termination of the Agreement with respect to circumstances arising prior to such termination.

9 Miscellaneous Provisions

- 9.1 Amendments.** This Agreement may not be amended, modified, altered, or supplemented other than: (a) with respect to the general form of the Agreement and non-Community-specific terms of the Agreement, by SEAL in its reasonable good faith discretion, with at least 45 days advance written notice prior thereto, published on SEAL's website and major social media accounts; or (b) with respect to Protocol-Community-specific terms of the Agreement, by the DAO Adoption Procedures, and then solely as to the particular Protocol Community utilizing such Adoption Procedures.
- 9.2 Costs of Agreement.** Each Party must pay its own fees, costs and expenses incurred by it in connection with that Party's review and participation in this Agreement and any transactions contemplated by this Agreement including without limitation legal, accounting, and other fees.
- 9.3 Entire Agreement.** This Agreement and the other agreements referred to herein set forth the entire understanding of the Parties hereto relating to the subject matter hereof and **thereof** and supersede all prior agreements and understandings among or between any of the parties relating to the subject matter hereof and thereof.
- 9.4 Further Assurances.** Whitehat shall execute and cause to be delivered to Protocol **Community** such instruments and other documents, and shall take such other actions, as Protocol Community may reasonably request for the purpose of carrying out or evidencing any of the matters contemplated by this Agreement.
- 9.5 Governing Law.** This Agreement shall be governed by and construed and interpreted in accordance with the laws of Singapore in the jurisdiction of the Singapore International Commercial Court. irrespective of the choice of laws principles thereof, as to all matters, including matters of validity, construction, effect, enforceability, performance and remedies.
- 9.6 Notices.** Any notice or other communication required or permitted to be delivered to any Party under this Agreement shall be in writing and shall be deemed properly delivered, given and received: (a) if delivered by hand, when delivered; (b) if sent on a business day by email transmission before 11:59 p.m. (recipient's time) on the day sent by email and receipt is confirmed, on the date on which receipt is confirmed; (c) if sent by **registered**, certified, or first class mail, the

third business day after being sent; and (d) if sent by overnight delivery via a national courier service, two business days after being delivered to such courier, in each case to the mailing address or email address set forth beneath the name of such Party below (or to such other mailing address or email address as such Party shall have specified in a written notice given to the other parties hereto):

If to Protocol Community:

To all (or as many as reasonably practicable, but in no event less than one) of the individuals or entities with `names` in the `Contact[] contactDetails` struct set during the DAO Adoption Procedures, in accordance with their respective `contact` details in such struct.

If to Whitehat:

In relation to a particular attempted or completed Eligible Funds Rescue, by sending a message to any address that could reasonably be believed to have been utilized by and under the control of the Whitehat in connection with such attempted or completed Eligible Funds Rescue.

- 9.7 Order of Precedence.** Where there is any ambiguity between the terms of this Agreement, the Summary (both at the commencement of this Agreement and forming part of the Schedule), and any other content displayed as part of the Protocol or communications between the Protocol Community (including the proposal adopting this Agreement) and any Whitehat, the terms of this Agreement will take precedence and prevail to the extent of any such ambiguity.
- 9.8 Parties in Interest.** None of the provisions of this Agreement is intended to provide any rights or remedies to any employee, creditor, third-party beneficiary, or any other Person other than Protocol Community, Protocol Community Members, Whitehat and their respective successors and assigns (if any).
- 9.9 Remedies Cumulative; Specific Performance.** The rights and remedies of the Parties hereto shall be cumulative (and not alternative). The parties to this Agreement agree that, in the event of any breach or threatened breach by Whitehat of any covenant, obligation or other provision set forth in this Agreement: (a) Protocol Community shall be entitled, without proof of actual damages, (in addition to any other remedy that may be available to it) to: (i) a decree or order of specific performance or mandamus to enforce the observance and performance of such covenant, obligation or other provision; and (ii) an injunction restraining such breach or threatened breach; and (b) Protocol Community shall not be required to provide any bond or other security in connection with any such decree, order or injunction or in connection with any related action or Legal Proceeding.
- 9.10 Severability.** In the event that any provision of this Agreement, or the application of any such provision to any Person or set of circumstances, shall be determined to be invalid, unlawful, void,

or unenforceable to any extent, the remainder of this Agreement, and the application of such provision to Persons or circumstances other than those as to which it is determined to be invalid, unlawful, void, or **unenforceable**, shall not be impaired or otherwise affected and shall continue to be valid and enforceable to the fullest extent permitted by law.

9.11 Successors and Assigns. This Agreement shall be binding upon and inure to the benefit of the parties, the Indemnitees, and their respective successors and assigns (if any). Protocol Community may freely assign any or all of its rights or delegate any or all of its **obligations** under this Agreement, in whole or in part, to any other Person without obtaining the consent or approval of any other party hereto or of any other Person. Whitehat shall not assign any of its rights or delegate any of its obligations under this Agreement, in whole or in part, to any other Person without the prior written consent of Protocol Community.

9.12 Taxation. Except as provided in Section 3.2(b)(i), each Party is liable for the payment of any income or capital gains taxation that such Party is liable to pay, and is solely responsible for otherwise complying with all tax-related legal and regulatory requirements applicable to such Party, as a result of the transactions contemplated by the Agreement. Except as provided in Section 3.2(b)(i), no Party shall be obliged to withhold any amount in respect of taxation and any payments made are presumed to be inclusive of any applicable sales or value-added taxation sums.

9.13 Waiver. No failure on the part of any Person to exercise any power, right, privilege, or remedy under this Agreement, or part thereof, and no delay on the part of any Person in exercising any power, right, privilege, or remedy under this Agreement, or part thereof, shall operate as a waiver of such power, right, privilege, or remedy; and no single or partial exercise of any such power, right, privilege, or remedy shall preclude any other or further exercise thereof or of any other power, right, privilege, or remedy. No Person shall be deemed to have waived any claim arising out of this Agreement, or any power, right, privilege, or remedy under this Agreement, unless the waiver of such claim, power, right, privilege, or remedy is expressly set forth in a written instrument duly executed and delivered on behalf of such Person (or, in the case of a Protocol Community or Protocol Community Member, through the relevant Adoption Procedures); and any such waiver shall not be applicable or have any effect except in the specific instance in which it is given.

9.14 Waiver of Class-Action Rights. To the extent permitted by applicable law, each Party waives the right to litigate in court or an arbitration proceeding any dispute arising in connection with this Agreement or an Eligible Funds Rescue as a class action, either as a member of a **class** or as a representative or to act as a private attorney general.

9.15 Waiver of Jury Trial. Each of the Parties hereto hereby irrevocably waives any and all right to trial by jury in any action, suit or other legal proceeding arising out of or related to this Agreement or the transactions contemplated hereby.

10 Construction and Interpretation

10.1 In interpreting any Sections or clauses of this Agreement:

- (a) **Ambiguities.** The parties hereto agree that any rule of construction to the effect that *ambiguities* are to be resolved against the drafting party shall not be applied in the construction or interpretation of this Agreement.
- (b) **Best Efforts.** The “best efforts” of a Whitehat under this Agreement are the efforts that would be applied by a reasonable blockchain-based protocol security expert acting in good faith under the circumstances as measured by then prevailing industry best standards and practices.
- (c) **Dollar.** Any references in this Agreement to “dollars” or “\$” shall be to U.S. dollars.
- (d) **Gender; Etc.** For purposes of this Agreement, whenever the context requires: the singular number shall include the plural, and vice versa; the masculine gender shall include the feminine and neuter genders; the feminine gender shall include the masculine and neuter genders; and the neuter gender shall include the masculine and feminine genders.
- (e) **Headings.** The bold-faced headings and the underlined headings contained in this Agreement are for convenience of reference only, shall not be deemed to be a part of this Agreement and shall not be referred to in connection with the construction or interpretation of this Agreement.
- (f) **Hereof.** The terms “hereof,” “herein,” “hereunder,” “hereby,” and “herewith” and words of similar import will, unless otherwise stated, be construed to refer to this Agreement as a whole and not to any particular provision of this Agreement.
- (g) **Including.** As used in this Agreement, the words “include” and “including,” and variations thereof, shall not *be* deemed to be terms of limitation, but rather shall be deemed to be followed by the words “without limitation.”
- (h) **Knowledge.** A reference to the awareness or knowledge of a party is a reference to the actual knowledge, information, and belief of a party as of each time relevant to such party’s entry into, performance of, or claiming or enforcement of any rights or benefits under this Agreement.
- (i) **References.** Except as otherwise indicated, all references in this Agreement to “Sections,” “Schedules,” and “Exhibits” are intended to refer to Sections of this Agreement and Schedules and Exhibits to this Agreement.

EXHIBIT A

CERTAIN DEFINED TERMS

For purposes of this Agreement, the capitalized terms set forth on Exhibit A shall have the definitions that are ascribed to them below:

“Affiliate” means, with respect to any Person, another Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such first Person.

“Assets” means the crypto-assets transacted on or in connection with an Eligible Funds Rescue in relation to the Protocol.

“Claim” means all past, present and future disputes, claims, controversies, demands, rights, obligations, liabilities, actions and causes of action of every kind and nature (whether matured or unmatured, absolute or contingent, known or unknown, suspect or unsuspected, disclosed or undisclosed).

“Damages” means any loss, damage, injury, decline in value, lost opportunity, Liability, claim, demand, settlement, judgment, award, fine, penalty, tax, fee (including reasonable attorneys’ fees), charge, costs (including costs of investigation) or expense of any nature.

“Entity” means any corporation (including any non-profit corporation), general partnership, limited partnership, limited liability partnership, joint venture, estate, trust, company (including any limited liability company or joint stock company), firm or other enterprise, association, organization or entity.

“Governmental Entity” means any: (a) nation, multinational, supranational, state, commonwealth, province, territory, county, municipality, district or other jurisdiction of any nature; (b) federal, state, provincial, local, municipal, foreign or other government; (c) instrumentality, subdivision, department, ministry, board, court, administrative agency or commission or other governmental Entity, authority or instrumentality or political subdivision thereof; or (d) any quasi-governmental or private body exercising any executive, legislative, judicial, regulatory, taxing, importing or other governmental functions.

“Intellectual Property License” means any license, sublicense, right, covenant, non-assertion, permission, immunity, consent, release or waiver under or with respect to any Intellectual Property Rights or Technology.

“Intellectual Property Rights” means any and all rights in intellectual property and/or industrial property anywhere in the world, whether arising under statute, common law or otherwise.

“Legal Proceeding” means any action, suit, litigation, arbitration, claim, proceeding (including any civil, criminal, administrative, investigative or appellate proceeding), hearing, inquiry, audit, examination or investigation commenced, brought, conducted or heard by or before, or otherwise involving, any court or other Governmental Entity or any arbitrator or arbitration panel.

“Legal Requirement” means any: (a) federal, state, local, municipal, foreign, supranational or other law, statute, constitution, treaty, principle of common law, directive, resolution, ordinance, code, rule, regulation, judgment, ruling or requirement issued, enacted, adopted, promulgated,

implemented or otherwise put into effect by or under the authority of any Governmental Entity; or (b) order, writ, injunction, judgment, edict, decree, ruling or award of any arbitrator or any court or other Governmental Entity.

“Liability” means any debt, obligation, duty or liability of any nature (including any unknown, undisclosed, unmatured, unaccrued, unasserted, contingent, indirect, conditional, implied, vicarious, derivative, joint, several or secondary liability), regardless of whether such debt, obligation, duty or liability is immediately due and payable.

“Parties” means the Protocol Community, Protocol Community Members and Whitehats participating in the Program, to whom these Terms apply.

“Person” means any individual, Entity or Governmental Entity.

“Program” means the process set out in this Agreement to incentivize Eligible Funds Rescues whereby a Whitehat may seek to conduct an Exploit and transfer Tokens to the Asset Recovery Address as further detailed in this Agreement.

“Representatives” of a Person means such Person’s officers, directors, employees, agents, attorneys, accountants, advisors and representatives.

“SEAL” means the Open Security Alliance Inc., a Texas corporation.

“Technology” means any and all: (a) technology, formulae, algorithms, procedures, processes, methods, techniques, ideas, know-how, creations, inventions, discoveries, and improvements (whether patentable or unpatentable and whether or not reduced to practice); (b) technical, engineering, manufacturing, product, marketing, servicing, business, financial, supplier, personnel and other information and materials; (c) specifications, designs, industrial designs, models, devices, prototypes, schematics and development tools; (d) software, websites, content, images, logos, graphics, text, photographs, artwork, audiovisual works, sound recordings, graphs, drawings, reports, analyses, writings, and other works of authorship and copyrightable subject matter; and (e) databases and other compilations and collections of data or information.

EXHIBIT B

DAO PROPOSAL GUIDELINES

Note any Protocol-specific DAO Proposal procedures, such as sentiment checks, pre-proposal audit, etc.

DAO Proposal Components:

1. Title - Post each proposal with a clear title around its objective, matching or referencing a unique identifier of the proposal that was submitted on-chain or will be submitted on-chain (for example, IPFS hash of pinned text for a prospective proposal, or transaction hash of a submitted proposal), and should follow any applicable ordering/numbering/categorization of the Protocol DAO.

Ex.) [Proposal No. __] - Adopt Safe Harbor Agreement for Whitehats

2. Overview - Delineate the objectives of the proposal and what specific actions are being enacted (if on-chain governance) and suggested (for off-chain signaled actions). The summary should specify on-chain target contracts and methods, and off-chain agents/designees, and describe the motivation behind the proposal, including but not limited to the problem(s) it solves and the value it adds to the Protocol and Protocol Community.

Ex.) The Security Alliance has prepared a Safe Harbor Agreement for Whitehats (the “Agreement”) to incentivize and give comfort to whitehats rescuing digital assets from active exploits of decentralized technologies (i.e., on-chain protocols), and to provide a safe harbor for assets that are the subject of an exploit. The text of the Agreement is [located/hosted/pinned at ____]. This Proposal’s aim is to provide an on-chain indication of our Protocol Community’s agreement to the Agreement as of the date of successful passing and execution.

3. Specification – Technical and (if applicable) legal specifications around the Proposal’s intended effects and actions. Specify target method(s) and argument(s), and all necessary off-chain signaled effects, actions, key actors, and beneficiaries.
 - a. Exercise care in entering the target contract address, target method signature, and target method arguments/parameters; if applicable, consult the Protocol documentation.

Ex.) A successfully passed proposal will result in the Protocol and Protocol Community’s revocable adoption of the Safe Harbor Agreement for Whitehats. The target is as follows: [Insert applicable function signature and params]

4. Benefits – Describe the reasonable, intended benefits to the Protocol and Protocol Community of the proposal’s implementation in quantitative and qualitative terms.

Ex.) By adopting this Agreement, our protocol community would encourage Whitehats (as defined in the Agreement) to, pursuant to criteria set out in the Agreement, responsibly test, seek to penetrate, and otherwise exploit software which utilizes, incorporates, or is otherwise complementary to our protocol, and potentially receive a reward for conducting such exploits. Following our protocol community’s adoption, only those Whitehats who agree to the terms of the Agreement and act accordingly would therefore be eligible for rewards; this way, the specific

parameters of Eligible Funds Rescue and reward procedures are agreed in advance, so frenzied rescues and negotiations immediately after exploits can be substantially mitigated. Adoption of the Agreement could generally provide a strong complement to protocol audits for ongoing security.

5. Detriments – Disclose reasonably foreseeable harm, damages, risks, and liabilities to the Protocol and Protocol Community resulting from this proposal’s implementation in quantitative and qualitative terms.

Ex.) While the Safe Harbor Agreement for Whitehats has been drafted and reviewed by numerous developers and lawyers, it may have unintentional or unanticipated legal consequences, loopholes, or other deficiencies for the Protocol, Protocol Community, or Whitehats. The length and relative complexity of the Safe Harbor Agreement for Whitehats may deter otherwise willing Whitehats from engaging in activity that would be beneficial to the Protocol.

6. Summary of Options – Clearly and succinctly summarize the vote options on this Proposal, especially if the options are more inclusive than simply *For* or *Against*.

Ex.) *For: Adopt the Safe Harbor Agreement for Whitehats. Against: Take no action.*

7. Summary of Proposed DAO Adoption Procedures – State the proposed parameterization of the `adoptSafeHarbor` function call for the DAO Adoption Procedures

EXHIBIT C

SECURITY TEAM ADOPTION PROCEDURES

[] [INSERT NAME OF INDIVIDUAL OR ENTITY] hereby acknowledges and agrees to, and consents to be bound by the terms and conditions of, that certain Safe Harbor Agreement for Whitehats, adopted by the Protocol Community on [] (the “*Whitehat Agreement*”), available here [], as a “Security Team” and member of the “Protocol Community” thereunder. Without limiting the generality of the foregoing:

- the Security Team hereby consents to Whitehats attempting Eligible Funds Rescues of any and all Tokens deposited into the Protocol and the deduction of Bounties out of such Tokens to compensate Eligible Whitehats for successful Eligible Funds Rescues;
- the Security Team acknowledges and agrees that Tokens may be lost, stolen, suffer diminished value, or become disabled or frozen in connection with attempts at Eligible Funds Rescues, or that the functioning of the Protocol may be adversely affected; and
- the Security Team agrees to hold the other Protocol Community Members harmless from any loss, liability or other damages suffered by the Security Team in connection with attempted Eligible Funds Exploits under the Whitehat Agreement.

[ADD SIGNATURE BLOCKS]

EXHIBIT D
USER ADOPTION PROCEDURES

*TO BE ADAPTED AND INSERTED INTO THE TERMS OF SERVICE FOR ALL WEB APPLICATIONS
RELEVANT TO USING THE PROTOCOL:*

**User Agreement to be Bound By Agreement, Consent to Attempted Eligible Funds Rescues and
Payment of Bounties**

The User hereby acknowledges and agrees to, and consents to be bound by the terms and conditions of, that certain Safe Harbor Agreement for Whitehats, adopted by the Protocol Community on [.] (the “*Whitehat Agreement*”), available here [.], as a “User” and member of the “Protocol Community” thereunder. Without limiting the generality of the foregoing:

- the User hereby consents to Whitehats attempting Eligible Funds Rescues of any and all Tokens deposited into the Protocol by the User and the deduction of Bounties out of User’s deposited Tokens to compensate Eligible Whitehats for successful Eligible Funds Rescues;
- the User acknowledges and agrees that Tokens may be lost, stolen, suffer diminished value, or become disabled or frozen in connection with attempts at Eligible Funds Rescues, and assumes all the risk of the foregoing;
- the User acknowledges and agrees that payment of the Bounty as a deduction from User’s Tokens to an Eligible Whitehat may constitute a taxable disposition by the User of the deducted Tokens, and agrees to assume to all risk of such adverse tax treatment; and
- the User agrees to hold the other Protocol Community Members harmless from any loss, liability or other damages suffered by the User in connection with attempted Eligible Funds Exploits under the Whitehat Agreement.

EXHIBIT E

WHITEHAT RISK DISCLOSURES

Participation in the [FINAL NAME OF PROGRAM] (the “Program”) carries a high degree of consequential risk. You should carefully consider the risks described below together with information presented in the Summary of the Program available at [SUMMARY] and the version of the Program Agreement maintained by the protocol which you wish to engage in advance of engaging it under the terms of the Agreement. Also consulting tax and legal advisors in advance of participation is also strongly recommended.

Terms capitalized below are defined in the template Protocol Agreement found at [LINKOUT].

The Protocol Community must properly implement the Program for the Protocol you are targeting before you engage the Program

You should confirm that the Protocol Community has properly implemented the Program, including by reviewing the applicable Adoption Form, before participating in the Program. If the Program is not properly implemented, it is likely that some or all of the terms of the Program Agreement will be unenforceable, which could expose you to liability from claims from certain Protocol Community Members or other Users.

You are expected to have experience with and expert-level knowledge of blockchain systems and cybersecurity as a condition of your participation

Given the nature of the activities that you will perform by participating in the Program, you should be highly skilled as a cybersecurity professional and believe that you will likely be able to succeed in your attempted rescue of the Protocol. If you cannot make these commitments, you should seriously consider the potential risks before engaging in the Program, including the risk that you might inadvertently violate relevant laws or regulations by seeking to undertake an Eligible Funds Rescue.

Failing to notify the Protocol Community that you are attempting a rescue may block your ability to obtain the Reward

As provided for in the Program Agreement, you should notify the Protocol Community that you are engaging in the Program, proper ways to contact the Protocol Community will be provided in the Program Agreement.

Failure to successfully send all Returnable Assets to the Asset Recovery Address may prevent you from getting a Bounty

Certain Protocol Communities may require you to deposit all Returnable Assets to the Asset Recovery Address, and failure to do so could constitute a violation of the terms of the Agreement. Moreover, even if you put a lot of work into trying to save assets or succeed in recovering *most* of them, there is no guarantee that you will receive any sort of reward or compensation for your effort and time.

Legal proceedings ongoing, pending, or threatened against you may make you ineligible for the Program

If you are involved in any legal proceedings or think you may be before completing your obligations and receiving your Reward under the Program Agreement, you should not engage the Program.

You agree to follow certain procedures in case you become eligible for a Bounty and it is not delivered in a timely manner or the amount of the Bounty is disputed

The Protocol Agreement details resolution steps to be taken if there is disagreement over the Bounty amount; however, you will not be able to sue any other party to the Program Agreement because of this disagreement.

You will be responsible for any tax liability incurred as a result of receiving the Bounty

The Protocol Community will not assist you in filing or structuring the Bounty for tax treatment in a way not described in the Program Agreement. You should be familiar with your tax obligations in your local jurisdiction before engaging the Program.

This Program cannot protect you from incurring criminal, regulatory, or other liability as a result of your participation

Although the Program may shield you from certain claims brought by the Protocol Community and its Members, no contract is able to prevent or preempt criminal, regulatory, or other liability. Moreover, legal claims may still be brought against you by third parties, who are not subject to this Agreement and its release provisions.

No partnership or endorsement is formed among you and any member of the Protocol Community

The Protocol Community is not engaging you as a partner, agent, or contractor. No relationship beyond that arising from being a party to the Program Agreement is formed through participation in the Program.

Indemnity of Protocol Community, Members, Affiliates

In cases where members of the Protocol Community or their Affiliates incur liability to others as a result of your actions under the Program, you will indemnify (reimburse their expenses) those parties.

You agree to follow certain procedures in case there is a dispute about the Agreement

In case there is a dispute about the Program Agreement, you will not be able to sue any party to the Agreement. Instead, your dispute must be arbitrated in the jurisdiction of the Singapore International Commercial Court using the rules of the Singapore International Arbitration Centre.

The Agreement may not be enforceable in all jurisdictions or against all relevant persons.

The default jurisdiction of the Program is under the Singapore International Commercial Court. Although the Agreement is a legally binding contract, it cannot be guaranteed to be enforceable in all jurisdictions

or under all circumstances. Some people in the Protocol Community and some third parties may still have claims against you that cannot be released through this Agreement.

You understand that if you profit in any way other than the Bounty, you may incur significant risk of liability.

Profiting in other ways from conducting this Exploit may constitute securities or commodities manipulation or fraud and has been prosecuted in that fashion in the past. Engaging in fraudulent or manipulative conduct is not covered by the release of liability under this program.

EXHIBIT F PROTOCOL FAQ

Safe Harbor Agreement for Whitehats – Frequently Asked Questions

This document (“FAQ”) is meant to provide additional information to Protocol Communities about certain aspects of the Safe Harbor Agreement for Whitehats (“Agreement”). In the event of any conflict or inconsistency between the FAQ and the text of the Agreement, the text of the Agreement will govern. The information provided in the FAQ does not, and is not intended to, constitute legal advice.

Adoption and Initial Implementation

1. **What is a Protocol Community?** As defined in the Agreement, a Protocol Community is the set of key stakeholders with an interest in a blockchain-based protocol or similar decentralized technology. This group will typically include the DAO governing a protocol, DAO members and participants, protocol users, and any individual or group of individuals involved in securing the protocol.
2. **If most blockchain-based protocols are meant to be open and permissionless, then how does a Protocol Community adopt the Agreement?** Exhibits B, C, and D to the Agreement provide guidance on how various groups can adopt the Agreement. Given that decentralized technologies are being developed, governed, and used in new and innovative ways, the Security Alliance recommends that Protocol Communities are thoughtful about how they publicize, deliberate about, and adopt the Agreement. Protocol Communities should consult with legal counsel about the adoption process as needed. Protocol Communities should consider the possibility that individuals and entities involved in developing, governing, and using their protocol may each use different communication channels to coordinate and discuss the protocol. Protocol Communities should consider using all of these channels to provide these individuals and entities with opportunities to learn about the Agreement, discuss its adoption, and agree to its terms. For instance, Protocol Communities may want to consider using popular communication channels, like Twitter and Discord, to publicize the Agreement. Protocol Communities might also coordinate with any independent entities that provide user interfaces for their protocol to engage with users. For some Protocol Communities, these steps may be helpful for promoting engagement with the Agreement adoption process.
3. **Should the process of adopting the Agreement occur in public?** Yes, Protocol Communities are required by the Agreement to create an Agreement Fact Page that provides access to the materials associated with the adoption process. Protocol Communities should consider making all aspects of the adoption process public so that as many stakeholders as possible can engage with the process.
4. **What steps should a Protocol Community take to implement the program described in the Agreement?** As described in the Agreement, Protocol Communities should take the following steps to adopt the Agreement and implement the program described in it:
 - a. Protocol Communities should clearly disclose the parameters selected during the DAO Adoption Procedures. The Agreement is an open-source template that requires Protocol Communities to add certain details and make certain decisions before it is adopted. These required items include:

- i. Specifying the protocol or other decentralized technology that will be subject to the Agreement. This process might require drafting a list of technical assets that are within the Agreement's scope;
 - ii. Indicating the specific Protocol Safety Address where Whitehats will deposit assets that they recover;
 - iii. Deciding whether to use a third-party vendor, like a bug bounty program administrator, to facilitate payment of the Bounty;
 - iv. Deciding whether anonymous or pseudonymous Whitehats can participate in the program and collect a Bounty without identifying themselves to the Protocol Community. This decision will impact the extent to which the Protocol Community can perform diligence on the Whitehat in advance of their participation in the program or collection of the Bounty;
 - v. Deciding whether to perform sanctions diligence or other forms of diligence on Whitehats in advance of their participation in the program or their collection of the Bounty;
 - vi. Deciding the percentage of Returnable Assets to be paid to Eligible Whitehats as a Bounty, which may involve reviewing the payment amounts associated with a Protocol Community's existing bug bounty program, if any; and
 - vii. Deciding whether Whitehats will be permitted to deduct the Bounty themselves from the assets that they recover. This decision will limit the extent to which the Protocol Community can perform diligence on the Whitehat or assess their compliance with the Agreement before the Whitehat collects the Bounty.
- b. Protocol Communities may consider making additional determinations which, if made, should also be included in both the Adopting Addendum and on the Adoption Form. These additional determinations may include:
 - i. Deciding whether to impose any additional cap(s) on the Bounty paid in connection with an Urgent Blackhat Exploit, such as an aggregate cap equivalent to a US Dollar amount and above which payment will not be made to an Eligible Whitehat(s), or a fixed cap applicable to each Eligible Whitehat contributing to an Eligible Funds Rescue; and
 - ii. Incorporating other due diligence requirements on Whitehats that address the unique needs of the Protocol Community adopting the Agreement.
- c. Protocol Communities should consult with legal counsel in relevant jurisdictions about the specific legal risks and benefits of each of the choices described above because they may expose the Protocol Community or Protocol Community Members to legal or regulatory risk.
- d. As described above, Protocol Communities must make certain information about the adoption process publicly accessible. Protocol Communities should consider taking other steps to include different stakeholders in the process.

- e. Protocol Communities should also consider communicating to potential Whitehats whether there are any limits to the release provisions provided by the Agreement based on the Protocol Community's specific circumstances. For instance, a Protocol Community might take the position that the Agreement does not bind the Protocol's Users or other Protocol Community Members. Under that circumstance, the Protocol Community should consider notifying Whitehats that the release provisions might not protect them from claims brought by persons or entities who are not parties to the Agreement.
- f. Protocol Communities should consider the additional steps needed to implement the program. These steps may include, but are not limited to, coordinating with a bug bounty program administrator and creating internal organizational structures for administering the program.

Compliance with Applicable Laws and Regulations

1. How can Protocol Communities adapt the Agreement so that it complies with applicable laws and regulations? The Agreement is a template agreement that is meant to be adapted for use by sophisticated Protocol Communities around the world. Protocol Communities are encouraged to customize the parameters of the Agreement via the DAO Adoption Procedures parameter settings so that it conforms with the specific laws and regulations that apply to them and otherwise meets their particular needs.

2. Should Protocol Communities take any steps to ensure that their Bounty payments to Whitehats comply with international sanctions regimes? Yes, each participating Protocol Community is expected to comply with applicable sanctions obligations, and the Security Alliance recommends that Protocol Communities implement a risk-based approach to ensuring compliance with these obligations. For example, while Section 5.3 of the Agreement requires Whitehats to represent that they are not subject to any national or international sanctions regimes, in some jurisdictions, risk of sanctions violations may be increased where Whitehats are able to anonymously attempt an Eligible Funds Rescue and receive or retain Returnable Assets as a Bounty. This risk may also be heightened where the Protocol Community does not take other steps, such as conducting pre-payment diligence and instituting monitoring measures, to prevent payment to a sanctioned entity. The Security Alliance further recommends that Protocol Communities consult with legal counsel about how to address potential risks associated with the applicable sanctions regime(s) and to discuss what measures Protocol Communities may wish to take to comply with the applicable regime(s).

3. Should Protocol Communities make Whitehats aware of the risks associated with the Agreement and the program that it describes? Yes. The Agreement includes a list of risk disclosures in Exhibit E. Protocol Communities should consider adding or modifying those risk disclosures to account for any risks that are specific to their situation. These specific risks might address positions that law enforcement or regulators may take with respect to the program in particular jurisdictions. Protocol Communities should consult with legal counsel about these risks as needed.