TECHNICAL SUMMARY

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.

1 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).

2 CHECKLIST

- 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.

3 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.
  - 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.
  - 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.
  - 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**.

4 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.

5 REPRESENTATIONS AND WARRANTIES YOU MAKE AS A WHITEHAT

- 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.

6 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.

7 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.

8 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).

9 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: https://docs.google.com/document/d/1sTpU37r8JPEAsxG3Y-Rf0pWMOEumTc2_QijZbSpSRW0/edit#heading=h.7z81worfyiy

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.