Summary of Whitehat Safe Harbor Agreement

DISCLAIMER: You are responsible for reading the full agreement found in the Whitehat Safe Harbor Agreement. The following is only a plain English summary, and the full document takes precedence in case of any conflicts or inconsistencies. Be responsible and thorough - failure to understand the agreement or follow it correctly will not only nullify any protections, but may result in serious legal consequences.

MOTIVATION AND BACKGROUND

- The intention of this 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.
- A "whitehat" must be not only well-intentioned but also competent. While there is no formal standard, you should have some background experience in software engineering, security, and/or blockchain auditing. Hacking a protocol affects other people's money and can cause irreversible consequences, so is your duty to act ethically, exercise caution, and execute well.
- Provided that you do act competently and in good faith, and your actions could not be considered gross negligence, fraud, or misconduct (see full agreement for details), you will not be held liable for any damages. In addition, 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 the protocol agrees that you acted in accordance with its conditions, you may keep a reward, typically proportional to your transfers to the Asset Recovery Address (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 eligible exploits.
    - 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. The reward defaults to 10%, but may be adjusted or capped in a specific protocol agreement.
    - 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.
- **Make sure you trust the protocol.** If the protocol decides you've broken the agreement, it can refuse to pay your reward even if you've already completed the funds rescue. 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.
- You have thoroughly confirmed the protocol has accepted this agreement, by cross-checking the agreement fact page and the registry on the **correct blockchain at the correct address**

- 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 8.12

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 used 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 technical and legal terms used in the agreement.
- Exhibit B outlines the procedures by which a protocol and/or DAO can adopt the Agreement.
- Exhibit C defines the Security Team acting on behalf of a given protocol and indicates its intent to cooperate with whitehats.
- Exhibit D indicates consent to funds rescues and bounty payments on the behalf of protocol users.

Things you must <u>always</u> check:

- ☑ List of eligible and ineligible exploits
- ☑ The ARA address matches on both the Agreement Fact Page 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

How to Execute an On-chain White Hat Rescue Effectively

After discovering a potential smart contract exploit in the wild, the next steps are:

1.) Contemplate Responsible Disclosure vs. Exploit
2.) Simulate
3.) Responsible Transaction Propagation

Step 1 - Responsible Disclosure vs. Executing Exploit

Once you've gained an understanding of a protocol's vulnerability, you should decide early if the best approach is to responsibly disclose the issue to the project or actively exploit under the guidance of the rules outlined in **Safe Harbor Agreement for Whitehats & Summary .** While executing the exploit might seem like the best option, there are several considerations you should make prior to proceeding:

- **How likely is it someone else will find this in the wild?** Is it being actively exploited in a race? Or is the contract years old and unlikely to be actively inspected?
- **How much user funds will be destroyed in the execution of the exploit?** If conducting an exploit requires moving a TWAP, for instance, the fees on that movement could be significant and eat into the funds available to return to users.
- **Is the affected contract pausable or upgradeable?** It is possible the project will have a more elegant/effective solution for resolving the exploit.
- **Is the team reachable and responsive?**

Executing an exploit is a last ditch effort that should be the best choice when compared to the risks of waiting and should not be the primary reporting mechanism. If the risks of waiting are minimal, reporting to the project should be the preferred method of resolution.

Step 2 - Simulation

It is important to simulate the exploit prior to on-chain execution to allow for instantaneous execution, fully recovering all assets, when landing on-chain. If your exploit half-executes, but reverts due to logic issues that prevent full recovery**, it is likely other actors will notice the exploit strategy and run a version that works**, likely landing in the very next block. These

transactions are powered by *generalized front-runners*, bots that scan other transactions for profitable activity, blindly copying these strategies and executing the strategy themselves. To simulate your transactions, there are many methods, but two important features to consider: **simulation privacy** and **multi-transaction simulation**.

Simulation Privacy

For the same reason it is important to keep your exploit transactions private, it is equally important to trust your simulation endpoint not to act on the transactions you are testing. It is likely that well-known providers, like Infura and Alchemy, will not leak your simulation, but for extremely large rescues, it is recommended to use your own node. Aside from perfect simulation privacy, it is possible to add custom plugins/endpoints that could enable deeper or more powerful simulation features. **Be wary of untrusted third parties offering free, remote simulation APIs to help you with your exploit.**

Multi-transaction Simulation

If the exploit only requires a single transaction to execute, there exists a large number of RPCs for simulating your transaction:

- Standard eth_call
- Geth tracing-api's
- Commercial tools like Tenderly

However, if an exploit requires multiple transactions to execute in sequence, that will require special tooling, to either "fork" mainnet or use an API which supports an array of transactions. To fork Ethereum try:

- Hardhat
- Alchemy

To run a single API call with an array of transactions:

- Flashbots eth_callBundle (requires running geth fork or using Flashbots endpoint)
- Others?

Responsible Transaction Propagation

Now that you have a set of transactions which are likely to succeed, it is time to land these transactions on-chain **without being witnessed in the mempool first**. Most active blockchains are monitored by "generalized front runners", automated bots which very quickly read pending transactions and attempt to copy internal strategies to "steal" profits contained inside other transactions, if possible. These bots are able to detect multiple dependent transactions and contract deployments in order to replicate the profitability. Due to this:

It is extremely import to privately relay your transaction(s) to miners/validators