Simple Arrangement for Funding Upload

This Simple Arrangement for Funding Upload (the ***"SAFU"*** or ***"Arrangement"***) is provided by Tharsis Labs Ltd. (the ***"Team"***) to specify the post-exploit policy of active vulnerability in Evmos blockchain (as known as the **"Evmos Protocol"**), with chain ID of 9001 (the ***"Network"***), for white hat hackers (the ***"Hacker"*** individually and the ***"Hackers"*** collectively), particularly regarding the matters of rewards and distributions.

The Team reserves the right to make amendments to this SAFU as necessary to ensure fair and equitable arrangement of post-exploit policy.

1. **Exemption of Hacker Liability**

    1.1. **No legal action**. The Team will not pursue legal action against Hackers who act in accordance with this Arrangement regarding behaviors towards vulnerabilities found in the Network.

2. **Secured Fund Return & Reward**

    2.1. **Fund Return**. The Hacker shall transfer the total amount of exploited funds (the ***"Secured Fund"***) to the Dropbox Address (*as specified below*) within a period of 48 hours (the ***"Grace Period"***) from the time they acquire the tokens from the exploited vulnerability. In the event that the Hacker fails to make such transfer within the Grace Period, the Hacker shall be deemed to be in breach of this Arrangement and the Team reserves the rights of taking legal action against the Hacker.

    2.2. **Bounty Computation**. There is no minimum threshold of native tokens from the Network, in this case, EVMOS Tokens (the ***"Tokens"***) that shall be secured. Hackers that secure vulnerable funds are able to claim 5% (the ***"Bounty Percent")*** of the total funds secured up to a total of 750,000 Tokens (the ***"Bounty Cap"***)(the ***"Bounty"***).

    The total amount claimable by each Hacker is defined by the Bounty Percent and Bounty Cap using the following formula:

    amount_claimable = min(bounty_cap, amount_secured * bounty_percent)

    In the event of fund return by multiple Hackers for the same active vulnerability event, the pro-rata allocations of bounty rewards will be calculated based on the respective amount returned and will be distributed among the Hackers, in order to ensure that total potential bounty rewards do not exceed the established Bounty Cap, regardless of the order in which the fund transfer occurs.

    2.3. **Bounty Distribution**. The Hackers are not required to proactively file a claim to receive Bounty. The Bounty distribution will be processed by the Team during the next upgrade of the Network.

    2.4. **Pre-conditions to Bounty Entitlement**.

2.4.1. **KYC**. The Arrangement requires KYC/KYB (also known as "Know Your Clients / Know Your Business") to be done for all Hackers pursuing a bounty valued above US$ 1,000. The information required (photographic ID, utility bill) is assessed by Driftwood Advisory Services Ltd. (the ***"KYC Provider"***). Whitehats business entities will have to provide additional information (e.g., directors, owners). The KYC Provider may request further information at its sole discretion for compliance with applicable laws. Please anticipate that the KYC Provider might require documentation in English, or in certified translations to it. The collection and assessment of this information will be done by the KYC Provider.

2.4.2. **Malicious Exploitation**. Any person or entity found to have exploited vulnerabilities for malicious purposes will be not eligible for any bounty rewards hereunder.

3. Dropbox Address for Returning Funds

3.1. Dropbox Address. This Arrangement defines a Dropbox (address or smart contract) to which the Secured Fund should be deposited (***"Dropbox Address"***). The following Dropbox address is available on the Network for the Hackers to return the Secured Fund:

Dropbox Address in Bech32 Format:

evmos1c6jdy4gy86s69auueqwfjs86vse7kz3grxm9h2

Dropbox Address in Hex Format:

0xc6A4d255043ea1A2F79CC81c9940FA6433eb0A28

3.2. Address Derivation. The Dropbox address corresponds to that is not controlled by the Team or any individual. The module Dropbox address provided above is derived cryptographically from the first 20 bytes of the SHA256 sum for the "safu" string, using the following algorithm:

address = shaSum256([]byte("safu"))[:20])

3.3. Source Addresses. In the event of a Bounty Distribution, the Bounty for Hackers will be paid out from the account balance of the Dropbox address.

4. Out of Scope Project

4.1. Out of Scope Project. While the purpose of the Dropbox address is to primarily receive the Secured Fund, it can technically function as an address to receive tokens secured from other projects apart from the Evmos Protocol itself, including but not limited to other smart contract decentralized applications on Evmos (also known as the "Evmos native projects") or other ERC20 projects, that have been exploited by Hackers due to a vulnerability thereof but have no effective Simple Arrangement for Funding Upload program of their own (***"Out of Scope***

Project"). The hackers who have transferred the exploited funds from the Out of Scope Project to Dropbox are not entitled to claim any Bounty from the Team or Network under this Arrangement.

4.2. **Mediation Support**. Where there is any dispute between such hackers and the Out of Scope Project, the Team may serve as a mediator between the two parties.

4.3. **No Liability**. The Team will in no event be liable for: (1) any reward payout obligations of the Out of Scope Project to the Hackers; (2) any consequential, special or indirect losses or damages suffered by the Out of Scope Project as a result of or in connection with the vulnerability exploiting behaviors by Hackers.