

# Nexus Mutual Sherlock Bug Bounty Cover Terms & Conditions (the "Cover Terms")

## COVER TERMS

These Cover Terms, including any Annexes and Schedules, govern the use of the Sherlock Bug Bounty Cover. The Annexes and Schedules shall be deemed incorporated into and shall have the same force and effect as if set forth in full in the body of these Cover Terms. Accordingly, any reference to these Cover Terms shall include the Annex and Schedules. In the event of any inconsistency or conflict between the provisions of these Cover Terms, and the Annex, the provisions of the Annex shall prevail.

### **PART A: BUG BOUNTY SPECIFIC TERMS**

1. **Part A Covered Event:** Subject to clause 3 (Part A Exclusions) and these Cover Terms, Nexus Mutual *may* pay a Claim under these Cover Terms if, during the Cover Period, the Covered Member has had a Confirmed Critical Bug on an Approved Bug Bounty Program.
2. **Part A Claim Amount Calculation:** the Claim Amount shall be subject to the Cover Amount and calculated as follows:
  - i. the lesser of:
    1. 80% of the Critical Bug Bounty amount awarded for the bug; and
    2. 100% of the Critical Bug Bounty amount awarded for the bug, less 10% of the maximum amount payable under a High Bug Bounty, as per the Approved Bug Bounty Programs. *(This ensures that the Covered Member is responsible for paying at least 10% of the maximum High Bug Bounty payment when a Critical Bug Bounty payment is made).*
3. **Part A Exclusions:** This Cover does not cover any loss, damage, cost or expense of whatsoever nature arising out of or relating to:
  - a. Any payment made under the Sherlock Approved Bug Bounty Program where the bug is not classified as "Critical".
  - b. Any payment made under the Sherlock Approved Bug Bounty Program where Nexus Mutual has a reasonable doubt as to the classification of a bug report and the bug has not been through a 3rd Party Mediation Process. For the avoidance of doubt, this exclusion does not apply if a 3rd Party Mediation Process has been conducted and the bug has been classified as "Critical".
  - c. Any Critical bug classified under the Approved Bug Bounty Program approved during a period of boosted rewards or any other additional incentives exceeding the standard rewards.
  - d. Any Critical Bug Bounties paid from guaranteed reward pools.
  - e. Any Critical Bug Bounties paid for code that is not live in a production environment actively used by genuine users.

## **PART B: NATIVE PROTOCOL SPECIFIC TERMS**

4. **Part B Covered Event:** Subject to clause 6 (Part B Exclusions), the Mutual *may* approve a Claim made under this Cover if:
  - a. the Covered Member is a Designated Protocol Team Member, and during the Cover Period, the Designated Protocol loses Users' funds in excess of the Deductible as a direct result of the Designated Protocol failing from either:
    - i. a smart contract code bug or error resulting in unintended use of the Designated Protocol; or
    - ii. a sudden and widespread economic event that is clearly outside the normal or intended operation of the Designated Protocol and affects multiple users where the loss is caused by:
      1. Oracle Failure; or
      2. Oracle Manipulation; or
      3. Liquidation Failure; or
      4. Governance Takeovers.and
  - b. the Covered Member provides:
    - i. A technical analysis of the Covered Event demonstrating the cause of the loss and the extraction of funds from the Designated Protocol including references to the relevant blockchain transactions; and
    - ii. Sufficient Cryptographic Evidence which shows that both the purchasing address and the transferred address are owned by the same Covered Member, if the Cover NFT is transferred to a different blockchain address.  
and
  - c. the Designated Protocol has suffered a Material Loss.
5. **Part B Claim Amount Calculation:**
  - a. For a Claim resulting from clause 4(a)(i), the Claim Amount should reflect the loss actually incurred by the Covered Member less the Deductible, up to a maximum payment of the remaining Cover Amount.
  - b. For a Claim resulting from clause 4(a)(ii), the Claim Amount should reflect the loss actually incurred by the Covered Member in any two (2) hour period less the Deductible up to a maximum payment of the remaining Cover Amount.
  - c. Loss amounts are to be calculated:
    - i. using the Block immediately prior to the Block where the loss actually occurred, or for a Claim resulting from clause 4(a)(ii) the first Block following the end of the two (2) hour period; and
    - ii. after subtracting any Reimbursements; and
    - iii. using exchange rates from *coingecko.com* or if not available any other reputable crypto pricing data site.
6. **Part B Exclusions:** Covered Member will not be able to submit a Claim under these Cover Terms for:
  - a. Losses due to phishing, private key security breaches, malware, miner behaviour or any other activity where the Designated Protocol continues to act as intended.

- b. Losses where the Designated Protocol was deployed primarily for the purpose of submitting a Claim under this Cover and not for real usage by the User.
- c. Losses where the Designated Protocol Team Member uses any administrative controls in the Designated Protocol, including but not limited to pausing any Designated Protocol functions, that leads to loss of User funds.
- d. Losses occurring during the Cover Period if:
  - i. the event occurred before the Cover Period began; or
  - ii. a public bug disclosure or warnings related to the event were made for the Designated Protocol before the Cover Period began; or
  - iii. where a public bug disclosure or warnings related to the event were made for the parent protocol before the Cover Period began, and the Designated Protocol is a fork of that parent protocol.
- e. Losses resulting from movements in the market price of assets used in, or relied upon, by the Designated Protocol except for any losses caused by asset price movements where the price movement meets the definition of Oracle Failure under clause 4(a)(ii)(1) or Oracle Manipulation under clause 4(a)(ii)(2).
- f. Losses resulting from the de-peg of any asset that the Designated Protocol generates.
- g. Losses resulting from the Owners or Controllers of the Designated Protocol confiscating or stealing funds from Users in line with the permissions of the Designated Protocol irrespective of the individual or entity that has access to the private keys of the Owner or Controller accounts (*"rug pull" exclusion*).
- h. Losses due to the user interface or website errors where the Designated Protocol continues to act as intended.
- i. Losses due to the failure of any components of the Designated Protocol that are used to bridge assets from one blockchain to another.
- j. Losses that occur prior to the Cover NFT being transferred to another address unless it meets the criteria listed in clause 4(b)(ii).

## **TERMS AND CONDITIONS APPLICABLE TO PART A AND PART B.**

- 7. Claim Essentials:
  - a. Nexus Mutual *may*, subject to the Claim Assessors vote and these Cover Terms, make a payment of the Claim Amount subject to:
    - i. a maximum of the remaining Cover Amount; and
    - ii. the Covered Member submitting a Claim within the following timeframes, failure to do so will result in a termination of the right to claim under this Cover:
      - 1. Only after the Cool Down period; and
      - 2. During the Cover Period or Grace Period.
  - b. Cover ends when:
    - i. the full Cover Amount has been redeemed in Claims; or
    - ii. the Cover Period specified at purchase has ended;whichever is earlier.

8. REPRESENTATIONS AND WARRANTIES. By accepting these Cover Terms, the Covered Member represents and warrants that it is purchasing the Cover with full knowledge and acceptance of its terms and conditions without any reliance on any representation, warranty, advice or other statement by Nexus Mutual or any of its representatives or advisors regarding any legal, tax or accounting implications or requirements of the Cover.
9. NO BENEFIT TO THIRD PARTIES. Except as expressly set forth in these Cover Terms, none of the provisions in these Cover Terms shall be for the benefit of or be enforceable by any person other than the Covered Member.
10. REDEEMING THE CLAIM. Subject to the approval of a Claim as outlined in these Cover Terms, the Covered Member may redeem the Claim Amount within 30 days from the Claim approval date. Failure to do so will result in forfeiture of the Claim.
11. REIMBURSEMENTS. The Covered Member shall take all reasonable steps to preserve any rights to Reimbursement or other recovery against any third party in connection with any claim for any loss, and preserve Nexus Mutual's Reimbursement rights with respect thereto.
  - a. Upon approval and redemption of a Claim Amount, the Covered Member agrees and warrants to:
    - i. Promptly, and in any event no later than within 20 days, assign all rights over any Reimbursements, or rights to any Reimbursements to the Foundation; and
  - b. If assignment is not possible, allow the Foundation to pursue recovery on their behalf.
  - c. In no event shall the Covered Member waive any rights that could adversely affect Nexus Mutual's or the Foundation's ability to recover Reimbursement or exercise its assignment rights. Any amounts recovered by the Covered Member or by Nexus Mutual and/or the Foundation in connection with the exercise of its Reimbursement or assignment rights shall be applied as follows:
    - i. First, to reimburse Nexus Mutual for the Claim Amount paid by Nexus Mutual under this Cover and for any costs or expenses incurred in connection with such recovery; and
    - ii. Second, any remaining recovered amounts shall be paid to the Covered Member.
  - d. The Covered Member shall not retain any compensation that results in double recovery for the same loss. In the event that the total amount recovered from all sources (including the Claim Amount, Reimbursements, or other recoveries) exceeds the Covered Member's actual loss, the Covered Member must return the excess to Nexus Mutual and/or the Entity. .
12. OFFSETTING RECOVERIES. Any Claims under this Cover shall be reduced by any recoveries (including recoveries from any contractors, subcontractors, suppliers or any insurance policies or indemnities) actually paid to the Covered Member.
13. MISREPRESENTATION AND FRAUD. The Cover will be void if, whether before or after a Covered Event, the Covered Member has:

- a. willfully concealed or willfully misrepresented any material fact or circumstances relating to this Cover, the subject thereof, or the interest of a Covered Member.
  - b. made any attempt to defraud Nexus Mutual.
14. **SEVERABILITY**. If any provision or provisions of this Cover shall be held to be invalid, illegal, or unenforceable for any reason whatsoever, then the validity, legality and enforceability of the remaining provisions of this Agreement (including, without limitation, all portions of any paragraphs of this Cover containing any such provision held to be invalid, illegal, or unenforceable that are not themselves invalid, illegal, or unenforceable) shall not in any way be affected or impaired.
15. **TRANSFERABILITY**. This Cover is only valid if it is purchased by the Designated Project and becomes entirely void if it is transferred to another address that is not owned by the Designated Project. Sufficient Cryptographic Evidence must be provided that proves both the purchasing address and the transferred address are owned by the same Covered Member.
16. **ENTIRE AGREEMENT**. These Cover Terms and any applicable addendums, schedules, and Annexes constitute the entire agreement between the parties and no Member, or Nexus Mutual as a whole, shall be liable or bound to any other Member in any manner by any warranties, representations or covenants outside these Cover Terms, whether or not in writing, in relation to the subject matter of this Cover.

## **DEFINITIONS**

**"3rd Party Mediation Process"** means the process outlined here: [Sherlock Bug Bounty Dispute Resolution](#).

**"Annex"** means a supplementary document attached to the Members Smart Contract Data and forming part of the Cover, providing additional conditions, definitions, and further details relevant to the Cover.

**"Approved Bug Bounty Program"** means a Bug Bounty program run by the Designated Project on the Sherlock platform, where security researchers report bugs in the Designated Project's codebase or system in return for a reward based on the severity of the bug.

**"Block"** means computer files that store transaction data within a blockchain database. All information about blockchain transactions is gathered and recorded inside these blocks and every newly generated block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Once the data is validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated.

**"Bug Bounty"** means the reward offered by a Designated Project in exchange for the identification and reporting of bugs in its codebase or system under the terms of an Approved Bug Bounty Program.

**"Claim"** means a request by a Covered Member in accordance with these Cover Terms for reimbursement of a loss resulting from a Covered Event, subject to the Cover Amount and these Cover Terms.



**"Claim Amount"** means the amount requested by the Covered Member in respect of a Claim under these Cover Terms, subject to and capped at / limited by the remaining Cover Amount. The calculation methodology and further details on the Claim Amount are set forth in Part A and Part B respectively.

**"Claim Assessor"** means a Member who assesses a Covered Member's Claim under these Cover Terms.

**"Confirmed Critical Bug"** means any Critical bug as confirmed by the Designated Project and Sherlock platform.

**"Cool Down Period"** means a period of fourteen (14) days following the occurrence of the Covered Event, during which no Claims may be made. The duration of the Cool Down Period may be adjusted as specified in the Annex for individual agreements.

**"Cover"** means collectively the matters which are the subject of the discretionary cover provided by Nexus Mutual as set out in the Member Smart Contract Data and these Cover Terms.

**"Cover Amount"** means the maximum amount payable under the Cover, as specified in the Member Smart Contract Data. This Cover Amount applies across Part A and Part B collectively. The aggregate amount of all the approved Claim Amounts across Part A and Part B shall not exceed the Cover Amount.

**"Covered Event"** for the purposes of this Cover, a Covered Event shall mean any event explicitly described in Part A and Part B (Covered Event) of these Cover Terms, subject to their respective conditions and exclusions, collectively referred to herein as a Covered Event.

**"Covered Member"** means a Member that has purchased Cover and, where applicable, a former Covered Member. For the purpose of this Nexus Mutual Sherlock Bug Bounty Cover, the Covered Member is the Designated Project.

**"Cover Period"** means the period of time that a Covered Member is protected under this Cover, specified by the Covered Member when purchasing Cover and stated in the Member Smart Contract Data.

**"Critical"** means any security bug or defect that leads to a direct loss of funds without (extensive) limitations of external conditions where the loss of the affected party must be significant and as defined by the Designated Project on their bug bounty program, as approved and published on the Sherlock Platform (as specified in the Annex). In the event of any conflict between the conditions defined by the Designated Project and published on the Sherlock Platform, and the Annex, the provisions of the Annex shall prevail.

**"Cryptographic Evidence"** means cryptographic evidence required when the Cover NFT has been transferred after the Covered Event, consisting of sufficient cryptographic proof linking the sender and the receiver. This could include, but is not limited to, a cryptographically signed message from the sender referencing the receiver's address or other equivalent cryptographically signed evidence.

**"Deductible"** for the purposes of Part B means 5% of the Cover Amount.

**"Designated Project"** means any program listed on the Sherlock platform that has an associated Bug Bounty program, as described on [Sherlock's Bug Bounty Platform](#).

**"Designated Protocol"** means open source smart contract code marketed under one brand, running on one or more public blockchain networks including any directly linked layer two components but excluding the underlying blockchain network or networks and the related mining or consensus activities. Designated Protocol specifically excludes any user interfaces, including websites or any other interface that is used to interact with the Designated Protocol.

**"Designated Protocol Team Member"** means a person who is an active contributor to the development of the Designated Protocol.

**"Entity"** means CRS, Foundation or any other entity designated by Nexus Mutual.

**"Foundation"** means Terrapin International Foundation.

**"Governance Takeovers"** means an event where a malicious actor forces through a malicious upgrade to a Designated Protocol smart contract.

**"Grace Period"** means the period during the Cover Period or within thirty five (35) days following Cover Period ending during which the Covered Member may submit a Claim.

**"High"** means any security bug or defect that:

- causes a loss of funds but requires certain external conditions or specific states, or a loss is highly constrained; or
- breaks core contract functionality, rendering the contract useless or leading to loss of funds that's relevant to the affected party;
- is defined as High by the Designated Project in its Bug Bounty program, as approved and published on the Sherlock Platform (as specified in the Annex). Where no specific value for a High severity is specified, the maximum payable amount will be deemed to be 25% of the maximum Critical Bounty payment.

In the event of any conflict between the conditions defined by the Designated Project and published on the Sherlock Platform, and the Annex, the provisions of the Annex shall prevail.

**"Keeper"** means a decentralised network participant or automated agent (including but not limited to externally owned accounts, or bots) that monitors and executes predefined operational tasks or jobs on one or more smart contracts on the Designated Protocol.

**"Liquidation Failure"** means an event where:

- Keepers are unable to liquidate collateral backing unhealthy borrow positions, resulting in bad debt that is subsequently socialized and passed on to all lenders within the affected market; or
- Keepers liquidate collateral backing unhealthy borrow positions for an amount less than 80% of the fair realisable market value of the collateral, taking account of the prevailing market conditions.

**"Material Loss"** means a loss of funds where the Claim Amount after subtracting any Reimbursement and the Deductible, exceeds the gas related costs reasonably required to operate the contract.

**"Member"** means an individual or entity who has paid their Membership Fee and is entered in Nexus Mutual's register of members and, where the context requires, a former member.

**"Member Smart Contract Data"** means data held on the Ethereum Network in relation to a specific Member Address.

**"Nexus Mutual"** means Nexus Mutual DAO.

**"Oracle Failure"** means an event in which incorrect price feed data is used by the Designated Protocol's smart contracts, where:

- for stablecoin-related oracles, the error exceeds 1%; or
- for all other assets, the error exceeds 2.5%

and such incorrect data arises as a result of any of the following:

- a faulty oracle configuration; or
- a lack of proper safeguards to prevent an unauthorized party from providing pricing updates; or
- a fixed-rate oracle that is manually updated where the data is updated incorrectly; or
- an oracle's defined trigger parameters to provide updates to its price feed are met but the price feed fails to update a Designated Protocol's smart contracts.

**"Oracle Manipulation"** means an event where price feed data is deliberately corrupted and leads to a loss of funds in a Designated Protocol.

**"Owner or Controller"** means the blockchain address or addresses which have permission to upgrade, change or alter the Designated Protocol either in part or in full.

**"Reimbursement"** means any current, past, or future indemnification, reimbursement or recovery or right to indemnification, reimbursement or recovery of an approved and redeemed Claim made under the Cover, or promised to be made, or made available to Covered Members.

**"Schedule(s)"** means, where applicable, a schedule attached to the Member Smart Contract Data.

**"User"** means the end-user of the Designated Protocol.