

# **RITA AI Smart Contract Auditor**

## **Renewable Energy Token**

0x10b9dd394467f2cfbc769e07e88dc7e2c41b0965

Detailed Security Audit

# Critical Functions Check

| Issue Description  | Checking Status |
|--|-----------------|
| Compiler errors  | Passed          |
| Race conditions and Reentrancy, Cross-function race conditions | High Risk       |
| Possible delays in data delivery                               | Passed          |
| Oracle calls   | Passed          |
| Front running  | Passed          |
| Timestamp dependence   | Low Risk        |
| Integer Overflow and Underflow                                 | Low Risk        |
| Dos with Revert  | Low Risk        |
| Dos with block gas limit                                       | Low Risk        |
| Methods execution permissions                                  | Low Risk        |
| Economy model of the contract                                  | High Risk       |
| The impact of the exchange rate on the logic                   | Passed          |
| Private user data leaks  | Passed          |
| Malicious Event log  | Passed          |
| Scoping and Declarations                                       | Passed          |
| Uninitialized storage pointers                                 | Passed          |
| Arithmetic accuracy  | Low Risk        |
| Design Logic   | Passed          |
| Cross-function race conditions                                 | Passed          |
| Safe Open Zeppelin contracts implementation and usage          | Passed          |
| Fallback function security                                     | Low Risk        |
| Unsafe delegatecall usage                                      | Passed          |
| Unrestricted public functions                                  | Passed          |
| Potential infinite loops                                       | Low Risk        |
| High gas consumption operations                                | Low Risk        |
| Unsafe send/transfer usage                                     | Low Risk        |

# Risky Functions Details

## Function: reentrancy

Critical reentrancy vulnerability detected, risking multiple function calls during a single transaction

## Function: timestamp

Potential timestamp dependence detected, risking manipulation of block timestamps for malicious behavior

## Function: permissions

Potential insecure method execution permissions detected, risking unauthorized access

## Function: economy

Critical economy model issue with fees (tax, liquidity, charity) detected, may lead to unexpected behavior or exploitation

## Function: loops

Potential infinite loops detected, risking contract freezing or high gas costs

## Function: gas

Potential high gas consumption operations detected, risking transaction failures or DoS attacks

**Function: send/transfer**

Potential unsafe send/transfer usage detected, risking reentrancy or fund loss



This audit was conducted and prepared by RITA AI