STATEMENT OF WORK #3

Project: Security Services Retainer (Smart Contract Audit & Code Review)

THIS STATEMENT OF WORK ("**SOW**") is effective as of , by and between Halborn Inc. ("**Halborn**") and Phoenix DAO ("**Client**") and is deemed to be incorporated into that certain Master Services Agreement ("**MSA**") by and between Halborn and Client. Any capitalized term used but not defined herein shall have the meaning ascribed to such term in the MSA.

. Description of Services

In purchasing Halborn's Security Services Retainer ("Retainer"), Client can receive each of the following services set forth in the attached Appendix A ("Service Types"), subject to limitations set forth in Section V ("Fees; Payment Schedule").

Halborn will perform a smart contract and code review of the following repos:

Solana: https://github.com/umbra-defi/smart-program
ZK: https://github.com/umbra-defi/zk-cirtcuits

Commit ID:
Smart-Program: 788f2ddc3da96b7007d6e4c7c68c1e8da6d9055c
zk: bfb1a0c482dd73a422c5f1abb27e3833d5d24886

II. Halborn Responsibilities

There are two distinct types of deliverables as part of this Security Services Retainer. Depending upon the Services performed, Halborn may provide the following:

- **Verbal Status Updates**: Halborn will provide verbal status updates for major findings or as requested. Verbal status updates will include findings to date, activities completed, plans for the next reporting period, and issues requiring attention.
- **Reports and Design Documents**: Following the completion of a Service set forth in Appendix A Halborn will provide the following deliverable:
- **Reviews and Assessments**: A report outlining the findings identified while performing technical and security assessments along with finding severity analysis and risk scoring, and recommended solutions to address the identified findings.

III. Kickoff and Notification

For every Service, Halborn will, with Client's participation, conduct an initial kickoff to review Client's primary focus and objectives under the Service. Client and Halborn will identify key activities, with associated prioritization. Subsequent requests by Client to obtain any of the Services shall be provided in writing by sending an email to the designated Halborn email address, which will be provided to Client at kickoff, or communicated to Halborn via mutually agreed communication platform.

IV. Timeline and Term

Services Start Date: January TBD 2026

Services End Date: February TBD 2026

Client acknowledges that Start Date is flexible, as it is contingent upon Client's approval of this SOW, receipt of payment for Fees, and delivering to Halborn related documents or material in scope of this SOW. Further, and to provide additional clarity on Start Date, Halborn generally commences the Services outlined in this SOW within fifteen (15) business days of the Start Date.

This agreement shall remain in effect for a period of one (1) year from the Effective Date (the "Initial Term") unless earlier terminated in accordance with the MSA. Upon the expiration of the Initial Term, this agreement will be renewed for subsequent one (1) year periods (each a "Renewal Term") upon mutual written consent of the parties.

V. Fees; Payment Schedule

Client agrees to pay Halborn $150,000 for a total of 50 work days of services ($3000 per day). Payment is due as follows: $100,000 is due net 5 days upon receipt of invoice, $50,000 will be due on the delivery of the draft report.

[Signature Page Follows]

IN WITNESS WHEREOF, the Parties hereto have executed this SOW as of the date set forth in the recitals.

CLIENT	HALBORN INC.
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Email: _____	Email: _____

Halborn Sales Representative:

By: _____

Name: _____

Appendix A –Service Types

Service Type	Description
Software/System/Process Design Advisory	Assistance in or execution of a design exercise with elements of requirements engineering, readiness assessment, embedding security in the core design.
Technical/Security Review	Review of the architecture of a system or software, or process review based on existing documentation, architecture plans, source code, interviews with stakeholders and OSINT. The review can be performed from many angles and please see Appendix E (“Threat Modeling Methodology”) for the details on Halborn’s approach to preparing threat models.
Penetration Testing	Evaluate web applications for vulnerabilities, including flaws in development, configuration, deployment, upgrade process, API integrations, maintenance or third-party add-ons. Please see appendix C (“Penetration Testing Services Overview”) for more details.
Source Code Security Assessment	A review focused on identification of security issues, business logic flaws, non-functional bugs, major inefficiencies and bottlenecks in execution, and misalignments with reference source code specification and design requirements. Includes remediation recommendations, control enhancements, and strategic guidance to achieve code that adheres to quality standards and is free of vulnerabilities. Please see appendix B (“Source Code Security Assessment Services Overview”) for more details.
Mobile Application Security Assessment	Test and improve the security of mobile applications. Enumerate the attack surface, looking for vulnerabilities, misconfigurations, or logic flaws that lead to likely paths of compromise and/or the exfiltration of data. Please see appendix B (“Source Code Security Assessment Services Overview”) for more details.

Red Team Exercise	Review Client's attack surface on their exposed infrastructure and assets to determine whether there is evidence of unauthorized access or activity
Cloud Security Assessment	A targeted assessment and deep dive review of the security configuration specific to critical business services, including AWS, Microsoft Azure, or Google Cloud Platform and their SaaS providers such as GitHub, Cloudflare, Vercel, Okta and on premises machines such as data centers or worker's machines. Please see appending D ("Cloud Security Assessment Services Overview") for more details.

Appendix B- Smart Contract Security Assessment Services Overview

Description of Services

Halborn takes a holistic approach in conducting and delivering smart contract security review services. The team utilizes a blend of both static and dynamic analysis tools, enabling for a systematic and repeatable approach to our methodology. Halborn leverages automated security scanning tools along with direct, line-by-line manual code review of smart contract functions with business logic and arithmetic review of both internal and external contract calls.

Additionally, Halborn's approach and methodology takes into account numerous security frameworks (e.g. NIST Special Publications) and standards (e.g. ERCs and EIPs), and the team will look to identify any potential issues with code operation and execution within key business jurisdictions.

Halborn utilizes industry standard tooling for our assessment framework approach, depending on the type of services provided (security assessment/fuzzing/mutation testing/formal verification):

- Web3 SDKs
- Mainnet/testnet forks
- RPC Node infrastructure
- Invariant testing tools
- Fuzzing tools
- Formal verification tools

Halborn will collaborate with the client team to build out a testing plan for the code in scope. The testing plan will include a detailed list of test scenarios and the following metadata will describe every scenario in the plan:

- Assertion/property/invariant
- Scenario type
- Relevant smart contract
- Relevant function
- Evaluation result

- Verification method
- Relevance
- Preconditions
- Test steps
- Expected result
- Actual result
- Tester notes

The testing plan will cover security-relevant functional and non-functional requirements as defined by the client and derived by Halborn from the technical and business specifics of the project.

Halborn engineers will leverage hands-on experience, internal vulnerability databases and security knowledge bases, and open-source and commercial security and technology research papers to identify the standards followed, design patterns implemented, frameworks used, and dependencies imported to extend the testing plan by scenarios relevant to the context of the business logic.

Halborn engineers will research the business purpose of the project and will understand its context to identify the user stories, features and roles which affect the shortlisted requirements or are considered mission-critical by the client team. Example security scenarios relevant to the tokenization process are given below:

Security and Compliance:

- Only authorized users can issue or transfer tokens
- Operations are compliant with user authentication and access control policies.
- All transactions involving token issuance and transfers are correctly logged and can be audited
- Sensitive data related to token ownership and transactions are encrypted both at rest and in transit.
- Smart contract functions comply with specific regulatory requirements (like KYC, AML) before and after token issuance.
- The system can freeze or seize tokens in response to regulatory orders or detected fraudulent activities.

Market Dynamics:

- Tokens can be easily integrated and accepted by existing cryptocurrency exchanges and platforms-ERCs are followed.
- The platform can handle high volumes without latency issues or inaccuracies in order execution.
- The token burning process works as intended and impacts the market as expected.

Scalability and Performance:

- Tokens can function seamlessly across different blockchain platforms.
- The system is efficient in processing large batches of transactions for token issuance or transfers.
- The system prioritizes transactions correctly and the result of execution is not influenced by the position of a transaction in a block.
- The system scales as more transactions are processed and more participants are onboarded.

In the event the smart contracts in scope are upgradeable, Halborn engineers will extend the testing plan with tests covering the particularities of the proxy pattern implemented, examples of which are given below:

Transparent Proxy:

- Upgrade Authorization Test
- Storage Layout Compatibility Test
- Fallback Function Handling Test
- Proxy-Implementation Separation Test

Universal Upgradeable Proxy Standard:

- Upgrade Functionality Test
- UpgradeAndCall Functionality Test
- Self-Destruct Prevention Test
- Direct Interaction Prevention Test

Diamond Proxy:

- Facet Replacement Test

- Facet Authorization Test
- Multiple Face Coexistence Test
- Selective Functionality Exposure Test

The testing plan will evolve throughout the engagement as Halborn engineers study the code, learn the functionality and explore yet undiscovered execution paths.

Deliverables

1. Draft Report: a detailed document highlighting all findings identified in the review, along with remediation recommendations and references if needed. Also included will be informational items to help improve code functionality and efficiency. The report will contain an executive summary, risk rating methodology overview, and for each finding the report will outline its technical details, issue severity and categorisation, Proof of Concepts if applicable, and improvement opportunities to reduce an occurrence of exploitation. The report will include outputs from the automated tools utilised in the testing process. Should no findings be identified, a report will still be delivered with an overview of tests conducted, security analysis approach, scan/test outputs, and code coverage.
   This report can potentially contain open security issues and should be shared on a need-to-know basis only.
2. Final Report: Following the receipt of full and final feedback from Client on all findings listed in the Draft Report, Halborn will deliver an updated report including details of all remediation plans, patches, fixes and other actions Client took to address the reported findings.

Appendix C –Penetration Testing Services Overview

Description of Services

The at Halborn team utilizes a blend of both automated tooling and manual inspection and is able to effectively identify vulnerabilities related to business logic, functionality, authentication and authorization, permissioned and privileged user escalation. Halborn will seek to exploit weak or lacking security controls related to confidentiality, integrity, and availability. Halborn has conducted thousands of penetration tests covering web applications, mobile applications, DLT and network infrastructure, cloud components (including secure enclaves), and SDLC and CI/CD pipeline tooling.

Halborn will follow our methodology and follows the following steps with a focus on the listed areas below in the course of the penetration testing:

Information gathering

The information-gathering phase consists of gathering information about the systems in scope, including their purpose, functionality, documentation, endpoints, and authentication mechanisms. Understand the app's intended use and potential attack vectors.

It includes application and infrastructure footprinting, metafile leakage review, listing services, operating system functions, and fingerprinting. This step maps the in-scope systems to prepare for identifying exploitable vulnerabilities collectively.

Threat Modeling

The threat modeling phase serves to evaluate the types of threats that may affect the target apps that are in scope. The types of attacks and likelihood of these threats materializing serve to inform risk rankings/priorities that are assigned to vulnerabilities throughout the assessment.

The perspective of the testing (external/internal, authenticated/unauthenticated, black box/crystal box, etc.) is also identified to ensure the validity of vulnerabilities discovered. This phase of the assessment also includes manual review of the exposed endpoints, determining business

functionality of the endpoints, and identifying unauthenticated/authenticated endpoint attack surface.

Vulnerability Analysis

The vulnerability analysis phase will encompass the enumeration of all in-scope targets/applications at both the network layer and the application layer. The phase involves documenting and analyzing vulnerabilities discovered due to Information Gathering and Threat Modeling. This step includes the analysis of output from the various security tools and manual testing techniques.

In this phase, Halborn performs an in-depth security review with 2 stages:

- Automatic review: The systems in scope are audited using specialized tools/software to scan and examine the system for common security vulnerabilities and insecure practices. These tools employ various techniques, such as pattern matching, data flow analysis, and control flow analysis, to identify potential security risks.
- Manual review: The systems in scope are reviewed by Halborn security experts to identify security vulnerabilities and weaknesses. Unlike automatic security reviews, which rely on automated tools, a manual review involves a careful and in-depth examination of the systems by experienced security professionals

Exploitation

This phase involves taking all potential vulnerabilities identified in the previous phases of the assessment and attempting to exploit them as an attacker would. This helps to evaluate the realistic risk level associated with the successful exploitation of the vulnerability, analyze the possibility of exploit/attack chains, and account for any mitigating controls that may be in place.

Post Exploitation

After successful exploitation, analysis may continue, including infrastructure analysis, pivoting, sensitive data identification, data exfiltration, and identification of high-value targets/data. The information collected here is used in the prioritization and criticality ranking of identified vulnerabilities.

Furthermore, chaining different vulnerabilities can lead to proof-of-concept vulnerabilities with higher criticality.

Deliverables

1. Draft Report: a detailed document highlighting all findings identified in the review, along with remediation recommendations and references if needed. Also included will be informational items to help improve code functionality and efficiency. The report will contain an executive summary, risk rating methodology overview, and for each finding the report will outline its technical details, issue severity and categorisation, Proof of Concepts if applicable, and improvement opportunities to reduce an occurrence of exploitation. The report will include outputs from the automated tools utilised in the testing process. Should no findings be identified, a report will still be delivered with an overview of tests conducted, security analysis approach, scan/test outputs, and code coverage.
   This report can potentially contain open security issues and should be shared on a need-to-know basis only.
2. Final Report: Following the receipt of full and final feedback from Client on all findings listed in the Draft Report, Halborn will validate any fixes introduced as part of the remediation plan and deliver an updated report including details of all remediation plans, patches, fixes and other actions Client took to address the reported findings.