<div align="center">**Penetration Testing Agreement**</div>

Between:

- **Pentester:** Elijah Kofi Gbadago ("Pen tester" "Independent Pen tester")

- **Client:** ParoCyber ("Client" "Company")

This Penetration Testing Agreement ("Agreement") sets forth the terms and conditions under which the Pentester will provide penetration testing services to ParoCyber.

1. **Scope of Services**
    1.1. Elijah, the Pentester ("Pentester") will perform penetration testing services ("Penetration Test") in accordance with the mutually agreed Statement of Work (SoW) and Penetration Test Scoping Form.
    1.2. The Penetration Test will evaluate the security posture of the Client's IT environment, focusing on the In-Scope Items defined in the State of Work (SoW).
    1.3. The Pentester will conduct testing using industry-recognized methodologies (e.g., Open Worldwide Application Security Project - OWASP, National Institute of Standards and Technology - NIST, Open Source Security Testing Methodology Manual - OSSTMM) and ethical hacking practices.
    1.4. The Pentester will provide evidence of findings and vulnerabilities discovered during testing, subject to confidentiality and sensitive information clauses.

2. **Client Responsibilities**
    2.1. The Client must provide accurate and complete information about In-Scope Items, including systems, IP ranges, domains, and applications.
    2.2. The Client must whitelist the Pentester's testing IP addresses on intrusion detection/prevention systems to avoid blocking legitimate test traffic.
    2.3. The Client must ensure that In-Scope Items remain stable and unchanged during the testing period.

2.4. The Client must not interfere with or attempt to manipulate the success or failure of the Penetration Test.

3. **Reporting**

    3.1. The Pentester will deliver a **Penetration Test Report** upon completion of testing. The report will include:

    - Executive summary of findings

    - Detailed technical issues with risk ratings

    - Documentation of vulnerabilities (CVEs, OWASP categories, etc.)

    - Recommendations for remediation

    - Conclusion and appendix

    3.2. For web application tests, the report will include an Open Worldwide Application Security Project Web Security Testing Guide (OWASP WSTG) table with relevant findings.

4. **Remediation and Re-Testing**

    4.1. Within 90 days of receiving the Penetration Test Report, the Client may request a re-test of remediated items.

    4.2. The Pentester is not responsible for remediation of identified issues unless separately contracted.

    4.3. If re-testing is performed, the Pentester will provide a **Re-Test Report** summarizing whether remediation was successful.

5. **Payment Terms**

    5.1. Service Fees will be invoiced as follows:

    - 50% of the agreed fee upon commencement of services

- 50% upon delivery of the Penetration Test Report

5.2. Additional services (e.g., remediation, extended testing) will be billed separately under a new agreement or amendment.

6. Confidentiality

6.1. All findings, reports, and sensitive information obtained during testing will be treated as confidential.

6.2. The Pentester will not disclose Client data to third parties without written consent, except as required by law.

7. Definitions

- **Approach Type:** Black Box, Grey Box, or White Box Testing, as defined in the SoW.

- **Black Box Testing:** Testing with no prior knowledge of systems, simulating real-world external attacks.

- **Grey Box Testing:** Testing with limited knowledge, including user accounts and system details.

- **White Box Testing:** Testing with full access to system documentation, source code, and configurations.

- **In-Scope Items:** Systems, IP addresses, domains, and applications identified in the SoW.

- **Penetration Test Report:** The formal document summarizing findings, risks, and recommendations.

8. Ethical Standards

8.1. The Pentester will adhere to professional ethical hacking standards, ensuring no harm to Client systems beyond agreed testing scope.

8.2. The Pentester will immediately notify the Client of any critical vulnerabilities discovered during testing.

9. **Termination**

9.1. Either party may terminate this Agreement with written notice if obligations are not met.

9.2. Upon termination, the Pentester will provide any completed work, and the Client will pay for services rendered up to the termination date.

10. Signatures

Pentester:

Name: _____

Signature: _____

Date: _____

Client (ParoCyber):

Name: _____

Signature: _____

Date: _____