Project - Pentesting Agreement

Document Version: 1.0
Date of Issuance: December 1, 2025

THIS AGREEMENT ("Pentesting Agreement") is entered into on December 1st, 2025, between Ebenezer Boateng Agyekum (hereinafter referred to as Pentester), with its principal place of business located at WBHA 12, Accra, and ParoCyber (hereinafter referred to as Client) with its principal place of business located at Mc Carthy Hill St, Accra.

1. Introduction and Objectives
This Statement of Work (SOW) outlines the scope, methodology, schedule, mutual responsibilities, and terms for a contracted Pentesting to be performed by the Pentester for the Client.

1.1. Goal of the Engagement:
The primary objective is to conduct an authorized, controlled security assessment to identify, validate, and report security vulnerabilities that could potentially compromise the confidentiality, integrity, or availability (CIA Triad) of the specified Information Systems of the Client.

1.2. Type of Assessment:
Gray Box Assessment: Testing will be conducted with limited, standard user credentials (e.g., standard login account) and some internal documentation of the client-facing system provided by the Client.

2. Scope of Work (Rules of Engagement)
This section rigidly defines the assets that are authorized for testing. Any target not explicitly listed below is deemed **OUT OF SCOPE.** The Pentester's activities must remain within the scope at all times.

2.1. In-Scope Assets:
Authorized testing is strictly limited to the following assets:

Asset Type	Target Name/Description
External Web Application	ParoCyber Training & Resource Portal
API Endpoints	Transactional & Authentication Service APIs
Public Network Range	Firewall & Edge Devices linked to the Portal

2.2. Out-of-Scope Assets (Explicit Prohibitions):
The Pentester is **strictly prohibited** from targeting the following:

- The Client's marketing website or any assets used for corporate finance or human resources.
- Any third-party or ancillary systems used by the Client (e.g., cloud storage, external payment gateways) unless explicit written consent is provided.
- Physical security assessments.
- Social Engineering against any employee, contractor, or vendor of the Client.
- All assets outside the network ranges/domains specified in Section 2.1.

2.3. Prohibited Testing Techniques:
The Pentester, agrees to use best efforts to ensure stability and will **NOT** utilize or attempt the following:

- **Uncontrolled Denial of Service (DoS/DDoS) Attacks**, including high-volume traffic flooding, stress testing, or similar methods that could lead to widespread service disruption. *Note: Controlled, low-impact rate-limiting tests for application resilience are permitted with prior notification.*
- The destruction, alteration, or deletion of data outside of the designated testing environments.
- Installation of any permanent malware, backdoors, or persistent remote access tools on the production environment.
- Any exploitation that propagates to, or targets, devices or users not within the defined scope.

3. Schedule, Communication, and Emergency Protocol
3.1. Testing Window:

- **Start Date & Time:** February 2, 2026, at 09:00 GMT
- **End Date & Time:** February 20, 2026, at 17:00 GMT
- **Testing Hours:** Testing activities are restricted to 09:00 to 18:00 GMT, Monday through Friday. No weekend or overnight testing is authorized without a separate, explicit addendum.

3.2. Primary Contacts:
All formal communications regarding the test, scope changes, or emergencies must be directed to the following Point of Contacts (POC) :

Party	**Name**	**Title**	**Phone Number**	**24/7 email**
Client POC	John Doe	Head of Security Operations	+123 00 000 0000	john.doe@sampleemail.com

Pentester POC	Ebenezer Boateng Agyekum	Independent Penetration Tester	+123 00 000 0000	john.doe@sampleemail.com

3.3. Emergency/Stop-Work Protocol:

- **Immediate Notification:** If any testing activity causes unexpected system degradation, service interruption, or the discovery of a vulnerability deemed **Critical Risk and immediately exploitable**, the Pentester **must immediately stop all active testing** and notify the Client POC via both phone and email.
- **Triage:** The Pentester will assist the staff of the Client to mitigate the immediate impact. Testing will only resume after the critical issue has been acknowledged and the Client POC has provided explicit written permission to continue.

4. Methodology and Deliverables

4.1. Methodology:

The assessment will follow industry-recognized standards, including the Penetration Testing Execution Standard (PTES) and the OWASP Testing Guide. Testing phases will include: Intelligence Gathering, Vulnerability Analysis, Exploitation, and Post-Exploitation (where authorized).

4.2. Deliverables:

Upon completion of the testing window, the Pentester shall provide the following deliverables:

- **Formal Penetration Test Report (PDF):** A comprehensive written report including an Executive Summary for leadership, Detailed Technical Findings with proof-of-concept evidence, severity ratings (leveraging the CVSS v3.1 framework), and tailored Remediation Recommendations.
- **Remediation Planning Session**: A one-hour remote video conference with the development and security teams of the Client to review the final report and discuss mitigation strategies.

5. Legal and Ethical Terms

5.1. Authorization and Indemnification:

The Client hereby warrants that they are the legal owner or authorized custodian of all assets specified in Section 2.1 and grants the Pentester, explicit, written consent to perform the outlined security assessment. The Client agrees to exempt the Pentester from liability for any damage or legal claims arising from authorized activities conducted in adherence to the scope of this SOW.

5.2. Confidentiality and Data Handling:
The Pentester agrees that all information accessed, discovered, created, or learned during the engagement—including vulnerability data, system information, and any collected credentials/hashes—is **Client Confidential Information** (CCI). This information shall not be disclosed to any third party, utilized, or retained by the Pentester after completion of the engagement, except as required by law. All collected data will be securely destroyed by the Pentester using industry-standard methods within **seven (7) calendar days** following the submission of the final report.

5.3. Ethical Conduct and Non-Disclosure:
The Pentester warrants that the assessment will be conducted in a professional, ethical, and controlled manner, adhering strictly to the scope and prohibited actions defined herein.

6. Compensation

Item	**Fee**	**Notes**
Penetration Testing Service (15-Day Engagement)	GH₵ 00,000.00	Includes execution of the test and final report generation.
Expenses (e.g., Licensing, Tools)	GH₵ 00,000.00	To be invoiced separately with receipts (e.g., API services).
Total Engagement Cost	**GH₵ 00,000.00**	**Payment Terms:** 50% retainer due upon signature; 50% balance due upon final report delivery.

7. **Term and Termination**
Unless terminated as provided herein, this Agreement shall extend to and terminate upon completion of Pentesting by Pentester as provided herein. Client may terminate this Agreement without cause upon thirty (30) days written notice. In the event of termination without cause, Client agrees to pay Pentester for all of Pentesting performed up to the date of termination. Either party may terminate this agreement for material breach, provided, however, that the terminating party has given the other party at least 15 days written notice of and the opportunity to cure the breach. Termination for breach shall not preclude the terminating party from exercising any other remedies for breach.

IN WITNESSES WHEREOFF, the parties hereto have executed this Pentesting Agreement as of the first date above written.

SIGNATURES

Signed

_____

John Doe,
ParoCyber
December 1, 2025

Signed

_____

Ebenezer Boateng Agyekum
Independent Penetration Tester
December 1, 2025