

PENETRATION TESTING AGREEMENT

This Penetration Testing Agreement (“Agreement”) is entered into on 04 December 2025, by and between:

- 1. ParoCyber (“Company”), with principal place of business at: Accra, Ghana
- 2. Stephen Jude (“Pen tester”), an independent security researcher/consultant, located at: Lagos, Nigeria.

Collectively referred to as the “Parties.”

1. PURPOSE

The purpose of this Agreement is to authorize the Pentester to conduct a controlled penetration test (“Pentest”) to identify security vulnerabilities in systems owned or managed by the Company, performed in accordance with global cybersecurity, legal, and ethical standards.

2. SCOPE OF WORK (SoW)

2.1 InScope Assets (Checkbox Style)

The following systems are authorized for testing. The Company shall check or enter all that apply.

Web Applications

- a) ☐ www.paro cyber.com
- b) ☐ portal.paro cyber.com
- c) ☐ Admin panels
- d) ☐ Other: _____

APIs / Backend Services

- a) ☐ REST API (api.paro cyber.com)
- b) ☐ Microservices
- c) ☐ GraphQL Services
- d) ☐ Other: _____

Mobile Applications

- a) ☐ Android App (APK provided)
- b) ☐ iOS App (TestFlight access)
- c) ☐ Other: _____

Network Infrastructure

- a) ☐ Internal IP Range(s): _____
- b) ☐ External IP Range(s): _____
- c) ☐ VPN Segment(s): _____

Cloud Resources

- a) ☐ AWS
- b) ☐ Azure
- c) ☐ Google Cloud
- d) IAM Roles Required: _____

Other Testing

- a) ☐ Social Engineering (phishing) — Requires express written approval
- b) ☐ Physical Security Testing — Requires express written approval
- c) ☐ Wireless Security
- d) ☐ Other: _____

2.2 Permitted Testing Activities

- Vulnerability scanning
- Manual exploitation (nondestructive)
- OWASPbased web and API assessment
- Cloud misconfiguration and IAM weaknesses
- Network enumeration & privilege escalation tests

- Secure configuration review

2.3 Prohibited Testing Activities

Unless explicitly approved in writing:

- DoS / DDoS attacks
- Ransomware or destructive payloads
- Extraction of large volumes of data
- Attacks on thirdparty systems
- Access to sensitive personal, medical, or financial data
- Physical intrusion or badge cloning

3. RULES OF ENGAGEMENT

3.1 Duration

The Penetration Testing engagement will last three (3) weeks from the official start date defined by the Parties.

3.2 Communication Protocol

Primary POC (Company): ParoCyber

Email: parocyber@gmail.com

Primary POC (Pentester): JayTech

Email: judestephen108@gmail.com

Critical findings must be reported immediately. A final report will be provided at the end of the engagement.

3.3 Safety Requirements

The Pentester agrees to:

- Avoid causing operational disruption
- Stop testing if instability is detected
- Maintain complete logs of testing activities
- Follow industry standard methodologies: NIST SP 800115, OWASP, CREST

4. LEGAL AUTHORIZATION

- The Company grants the Pentester explicit legal permission to perform security testing on the assets defined in Section 2.
- The Pentester is protected from unauthorized access claims as long as all activities remain within scope.

5. GDPR & DATA PROTECTION CLAUSES

5.1 Data Processor Role

- The Pentester acts solely as a Data Processor when handling any personal data during the test.

5.2 Data Minimization

- The Pentester will collect only what is required to demonstrate vulnerabilities and will pseudonymize or redact data where possible.

5.3 Lawful Basis

- The Company confirms it has a lawful basis (GDPR Art. 6) to authorize penetration testing.

5.4 Breach Notification

- Any accidental exposure of personal data must be reported to the Company within 12 hours.

5.5 Data Retention

- All sensitive data will be securely deleted within 7 days of final report delivery.

6. CONFIDENTIALITY

- The Pentester shall not disclose any Company data, credentials, vulnerabilities, or findings to third parties without written consent. Confidentiality obligations survive indefinitely.

7. DELIVERABLES

The Pentester will provide:

1. Testing Plan / Engagement Overview
2. Daily or Periodic Updates (if required)
3. Final Penetration Test Report including:
 - a. Executive Report
 - b. Technical Findings
 - c. CVSS Severity Scores
 - d. Proofofconcept evidence
 - e. Remediation guidance
4. Retest Report (if contracted)

8. PAYMENT TERMS

Total Fee: \$35,000

Payment Schedule:

- 70% (\$24,500) before testing starts (nonrefundable)
- 30% (\$10,500) after delivery of the final report

Invoices are due within 15 days.

Additional services (retesting, consulting, extra assets) may incur additional fees.

9. LIABILITY & INDEMNIFICATION

9.1 Pentester Liability Limits

The Pentester is not responsible for:

- Preexisting vulnerabilities
- System failures due to outdated or misconfigured infrastructure
- Issues unrelated to testing
- Thirdparty service outages
- Liability is limited to the total fees paid under this Agreement.

9.2 Company Liability

The Company agrees to indemnify the Pentester against:

- Claims arising from unauthorized asset ownership
- Damages due to inaccurate scope assignment
- Thirdparty complaints resulting from Company misrepresentation

9.3 Force Majeure

- Neither party is liable for delays caused by events beyond their control.

10. TERMINATION

- Either Party may terminate the Agreement with written notice.
- Fees for completed work remain payable.
- Immediate termination applies for unlawful activity, scope violation, or breach of contract terms.

11. INTELLECTUAL PROPERTY RIGHTS

- The Pentester retains ownership of all tools, techniques, and methodologies.
- The Company receives a license for internal use of the final report only.

12. GOVERNING LAW

This Agreement is governed by the laws of Ghana, unless mutually amended in writing.

13. SIGNATURES

IN WITNESS WHEREOF, the Parties execute this Agreement as of the date first written above.

For ParoCyber (Company)

Name: _____
Title: _____
Signature: _____
Date: _____

For Stephen Jude (Pentester)

Name: _____
Title: _____
Signature: _____
Date: _____