Penetration Testing Agreement

This Penetration Testing Agreement (“Agreement”) between ParoCyber (Client) and the Independent Penetration Tester (Service Provider) is entered into on 2 December 2025, by and between:

Client:
Name: ParoCyber
Address: McCarthy Hill - Accra, Ghana
Email: parocyber@gmail.com
Phone: +233509811131

Service Provider:
Name: Shuseel Baral
Address: Pokhara, Nepal
Email: b********@gmail.com
Phone: +977**********

Collectively referred to as the “Parties.”

1. Introduction

This Agreement governs the responsibilities, scope, and obligations between the Client and the Service Provider for ethical penetration testing services.

2. Purpose

The purpose of this Agreement is to authorize and govern penetration testing services to identify and mitigate potential vulnerabilities in the Client’s systems and infrastructure.

3. Scope of Work

3.1 The testing will cover the following:

- Networks: IP ranges include 172.24.1.0/24 and 172.25.0.0/16, with a server at 172.16.1.0, and the routers in the network.
- Applications: Mobile apps (both Android and IOS versions) and the API “api.parocyber.com/v2.”
- Physical security: Security of the Network devices
- Social engineering attempts (limited to the provided email addresses).

3.2 The service provider agrees to:

- **Follow Ethical and Legal Standards:** Ensure all testing activities comply with applicable laws, industry standards, and ethical guidelines. No actions will be taken outside the agreed scope without prior written consent.

- **Minimize Operational Impact:** Use safe testing methodologies to avoid unnecessary disruption of client systems, services, or data.

- **Report Vulnerabilities Promptly:** Immediately notify the client of any critical vulnerabilities or exposures that pose imminent risk to business operations or sensitive data.

- **Provide Deliverables:** Deliver a comprehensive report including:
    - Executive summary of findings
    - Detailed technical descriptions of vulnerabilities discovered
    - Proof-of-concept evidence (where appropriate)
    - Risk ratings and prioritization
    - Recommended remediation steps

3.3 The Client Agrees to:

- Provide Written Authorization to obtain and furnish all necessary consent documents, including authorization letters, to ensure testing activities are legally sanctioned.
- Supply accurate details of systems, applications, and environments to be tested, and confirm exclusions to avoid unintended impact.
- Back up all critical data and ensure disaster recovery procedures are in place before commencement of testing.
- Provide the service provider with appropriate access credentials, network information, and physical accommodations (if required) to perform the agreed tests.
- Assign a responsible representative to coordinate with the penetration tester, receive updates, and respond to urgent findings.
- Review the final report, prioritize remediation efforts, and implement corrective measures in a timely manner.

3.4 Specific exclusions:

The Penetration Tester Will Not:

- Perform Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) Attacks. No stress testing or load testing that could intentionally disrupt client systems or services.
- Access or Alter Production Data Testing will avoid modification, deletion, or corruption of live production data. Any data used for testing will be anonymized or provided by the client.
- Exploit Vulnerabilities Beyond Proof-of-Concept. Vulnerabilities will be demonstrated only to the extent necessary to validate their existence. Full exploitation, data exfiltration, or privilege escalation beyond agreed limits will not be performed.

- Any systems, applications, or environments not explicitly listed in the agreed scope are excluded from testing.
- Social engineering activities (e.g., phishing, pretexting, impersonation) will only be conducted if explicitly authorized in writing by the client.
- Physical penetration tests (e.g., facility access attempts) will only occur if specifically included in the scope and authorized by the client.
- The penetration tester will provide recommendations, but is not responsible for implementing or guaranteeing remediation of identified vulnerabilities.

4. Testing Schedule

- Start date: 15 December 2025
- End date: 14 January 2026
  Testing will occur during the following hours to minimize operational disruptions: 2 AM to 6 AM GMT from Sunday to Friday.

5. Methodology

The Service Provider shall conduct testing using recognized ethical hacking techniques and frameworks such as OWASP, NIST, or ISO standards.

No destructive or disruptive actions shall be taken without prior written consent.

6. Reporting

- A preliminary report will be provided within 15 days of test completion.
- A final comprehensive report, including vulnerabilities and remediation recommendations, will be delivered within 30 days.
- Reports shall be treated as confidential information.

7. Confidentiality

Both Parties agree to maintain strict confidentiality regarding all information accessed or disclosed during the engagement, including vulnerabilities, system data, and results.

Confidential information shall not be shared with third parties without prior written consent.

8. Legal Authorization

The Client grants explicit legal authorization to the Service Provider to conduct penetration testing as defined in this Agreement.

The Client assumes responsibility for securing any necessary third-party consents.

9. Liability Limitations

- The Service Provider’s liability is limited to the total fees paid under this Agreement.
- The Client agrees to indemnify the Service Provider against claims arising from the Client’s misuse of findings or failure to implement remediation steps.

10. Fees and Payment

- Total fee: $10000
- Payment terms: 40% due upon signing, 60% upon delivery of the final report, and late payments are subject to 2% interest per month.

11. Termination

Either Party may terminate this Agreement with 15 days written notice.

Upon termination, the Client shall pay for all work completed up to the date of termination.

12. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of Ghana.

13. Entire Agreement

This document constitutes the entire agreement between the Parties and supersedes all prior negotiations and agreements.

Signatures

Client Signature: ....
Client’s Name: ParoCyber
Date: 2 December 2025

Service Provider Signature: ....
Service Provider Name: Shuseel Baral
Date: 2 December 2025