PENETRATION TESTING AGREEMENT
Version 1.0

1. Introduction

This Penetration Testing Agreement ("Agreement") is made between:

Client: ParocyberGH
Pentester / Security Analyst: Edwin Atali
Date: 3rd December, 2025

The purpose of this Agreement is to define the scope, rules, permissions, and ethical boundaries governing an authorized penetration test ("Pentest") to assess the security posture of the Client's systems.

2. Objectives

The objectives of the Pentest include, but are not limited to:

Identifying vulnerabilities that could be exploited by attackers
Evaluating the effectiveness of existing security controls
Testing incident detection and response capabilities
Providing recommendations for risk mitigation

3. Scope of Testing

The authorized scope of this Pentest explicitly includes the following:

3.1 In-Scope Systems & Assets

Systems:
Applications:
Network ranges:
Cloud services:
APIs:
Physical locations (if applicable):

Only the assets listed above are authorized. Testing anything outside this scope is strictly prohibited.

3.2 Testing Methods Allowed

External network penetration testing
Internal network penetration testing (if access is provided)
Web application security assessment

API security testing
Social engineering (only if explicitly approved below)
Physical security testing (only if explicitly approved below)

Social Engineering ✓ Allowed ☐ Not Allowed
Physical Testing ✓ Allowed ☐ Not Allowed

4. Rules of Engagement

4.1 Testing Window
Start Date: 5th December, 2025
End Date: 5th February, 2026
Testing will occur between **approved business hours** unless otherwise authorized.

4.2 Safety Controls
The following actions are **prohibited** unless explicitly permitted:

Disrupting production systems
Denial-of-Service (DoS or DDoS)
Ransomware simulation
Data deletion, modification, or exfiltration
Exploiting vulnerabilities beyond proof-of-concept
Accessing sensitive personal data unless necessary for validation

4.3 Data Handling
All collected data will be securely stored and encrypted.
No data will be retained after the engagement ends (maximum 30-day retention).
Client data will never be shared with third parties.

5. Legal Authorization
The Client formally grants the Pentester **full legal permission** to perform the activities described in Section 3.
The Pentester is protected from legal action as long as:

All engagement rules are followed
The Pentester works within agreed scope
No malicious intent or misuse of access occurs

Unauthorized actions void this protection.

6. Reporting Requirements

At the end of the engagement, the Pentester will deliver:

Executive Summary Report
Technical Findings Report
Vulnerability Severity Ratings
Screenshots and POC evidence
Mitigation & remediation recommendations

Critical findings will be reported **immediately** upon discovery.

7. Confidentiality

Both parties agree to:

Maintain confidentiality of all information related to the engagement
Not disclose findings to external parties without written permission
Handle sensitive data in accordance with ethical and legal standards

8. Liability

The Pentester is not liable for:

Pre-existing vulnerabilities
System outages caused by fragile infrastructure
Client negligence or misconfigurations

The Pentester **is** liable for:

Actions outside scope
Intentional harm
Violating confidentiality or agreements

9. Payment Terms

Total fee for the engagement: GHS 15000.00
50% upfront (optional), 50% after final report
Payment method: Cheque

10. Signatures

Client Representative
Name: Parocyber
Signature:
Date:

Pentester / Consultant
Name: Edwin Atali
Signature:
Date:

End of Agreement