PENETRATION TESTING AGREEMENT

This Penetration Testing Agreement ("Agreement") is entered into between the following parties:

1. Parties to the Agreement

Client (ParoCyber)

Company Name: ParoCyber
Address: _____
City / Country: _____
Primary Contact Person: _____
Email: _____
Phone Number: _____

Consultant / Penetration Tester (You)

Full Name: Maria Sagwa
Business Name (if applicable): _____
Address: _____
City / Country: _____
Email: _____
Phone Number: _____

Both parties agree to the terms set forth below.

2. Purpose of the Agreement

This Agreement authorizes and governs a controlled cybersecurity assessment to be performed by the Consultant against systems owned or legally managed by ParoCyber ("Client"). The purpose of the engagement is to identify security weaknesses, evaluate exploitability, and provide actionable recommendations to strengthen the Client's security posture.

3. Scope of Services

3.1 Engagement Goals

The Consultant will:

- Assess vulnerabilities within the Client's authorized systems.
- Simulate real-world attack scenarios in a controlled and lawful manner.
- Evaluate potential risks to confidentiality, integrity, and availability.
- Provide a detailed Penetration Test Report and recommended remediations.

3.2 Testing Methodology

The assessment will follow a structured, industry-standard workflow:

1. Information Gathering:
   Passive and active discovery of the in-scope systems, services, network exposures, and relevant public data.
2. Vulnerability Analysis:
   Identification of weaknesses through manual inspection, configuration review, automated tools, and threat modeling.
3. Exploitation:
   Attempting to validate vulnerabilities through controlled exploitation, without disrupting system availability.
4. Post-Exploitation:
   Determining depth of compromise, privilege escalation potential, and impact of unauthorized access.
5. Documentation & Reporting:
   Summarizing findings, risk severity, and remediation steps.

3.3 Testing Approach

The Client will choose one of the following:

- Black Box: Minimal information provided; testing simulates an external attacker.
- Grey Box: Limited credentials or architecture details supplied.
- White Box: Full access to documentation and credentials to enable a comprehensive review.

3.4 In-Scope Assets

The following items constitute the authorized testing scope:

Systems, applications, IP ranges, domains, cloud resources, or networks explicitly listed in an attached Scope Appendix.

Any asset not listed is out of scope by default.

4. Client Responsibilities

The Client agrees to:

1. Ensure all target systems are legally owned or properly authorized for testing.
2. Provide accurate scope details (IP ranges, accounts, application URLs, cloud approval letters, etc.).
3. Notify relevant internal teams (IT, Security, SOC) to prevent mistaken incident escalation.
4. Maintain adequate data backups before testing.
5. Provide timely access or credentials required for Grey/White Box testing.
6. Inform the Consultant immediately if any instability or service degradation is observed.
7. Communicate scope changes only in writing; changes may affect scheduling and cost.

5. Consultant Responsibilities

The Consultant agrees to:

1. Perform testing professionally and in accordance with best practices (e.g., OWASP, NIST, PTES).
2. Minimize disruption and avoid unnecessary risk to Client systems.
3. Protect sensitive information accessed during testing.
4. Immediately report any critical vulnerabilities that pose significant risk.
5. Retain data only as long as needed for reporting, and securely delete it afterwards.
6. Conduct all activities strictly within the authorized scope.

6. Deliverables

6.1 Penetration Test Report

The Consultant will provide a comprehensive report that includes:

- Project overview & scope
- Testing methodology
- Executive summary of results
- Detailed technical findings with severity ratings
- Proof-of-concept descriptions or screenshots
- Prioritized remediation recommendations
- References (e.g., CVE, CWE, OWASP)
- An appendix containing supporting details

6.2 Retesting Option

Upon request, the Consultant may re-test previously identified issues after Client remediation. Retesting will be limited to vulnerabilities listed in the original report unless otherwise agreed.

7. Authorization & Safe Harbor

7.1 Legal Authorization

The Client formally authorizes the Consultant to perform the activities described in this Agreement. All actions performed within scope shall be considered authorized security testing.

7.2 Limitations

- The Consultant will not:
- Target systems not listed in scope
- Conduct denial-of-service (DoS) tests
- Exploit vulnerabilities in a destructive manner
- Access employee personal data beyond what is necessary
- Perform social engineering unless separately authorized

7.3 Safe Harbor Protection

The Client agrees not to pursue legal, civil, or administrative action against the Consultant for activities conducted within the agreed scope, even if such activities would otherwise violate laws related to unauthorized access.

8. Confidentiality

Both parties agree to:

- Treat all exchanged information as confidential
- Avoid disclosure to any third party without written consent
- Securely protect all sensitive information
- Minimize collection of unnecessary data during testing
- All evidence obtained during the penetration test will be sanitized where feasible.

9. Liability & Risk Acknowledgment

1. The Client acknowledges that penetration testing inherently involves risks, including potential system performance impact.
2. The Consultant will exercise reasonable skill and caution but cannot guarantee:
    - Identification of all vulnerabilities
    - Prevention of system outages resulting from pre-existing weaknesses
3. The Client remains responsible for system stability, data backups, and operational continuity.
4. The Consultant's liability shall be limited to the total fees paid under this Agreement, unless prohibited by law.

10. Fees & Payment Terms

- Project fees will be agreed upon in the Statement of Work (SOW).
- 50% payment is due at project start; 50% upon delivery of the final report (unless otherwise agreed).

- Additional services (e.g., expanded scope, emergency testing, extensive retesting) will incur separate fees.

11. Termination

Either party may terminate this Agreement if:

- The other party violates material terms
- Legal constraints prevent continued testing
- Scope ownership or authorization cannot be verified

Upon termination:

- The Consultant will cease all testing immediately
- All collected data will be deleted or returned at Client's request

12. Governing Law

This Agreement shall be governed by the laws of Kenya , without regard to conflict-of-law principles.

13. Signatures

Client: ParoCyber
Name: _____
Title: _____
Signature: _____
Date: _____

Consultant (Pentester): [Your Name]
Signature: _____
Date: _____