ParoCyber

Penetration Testing Engagement

Penetration Testing Agreement

ParoCyber ↔ Pentester

Engagement ID: PCL-PTA-2025-0123
Period: 09–20 Dec 2025
Prepared by: Bryan M Nturibi (Independent Pentester)

Effective Date: 08 December 2025

Agreement No.: PCL-PTA-2025-0123

1. Parties

Pentester (Contractor): Bryan M Nturibi — ID/Passport: 123456; Email: bryan.nturibi@example.com; Phone: +254-700-000000; Address: Riverside Park, Suite 4xx

Client: ParoCyber Ltd — Company Reg: PCL-2023-00123; Email: security@parocyber.example; Phone: +254-711-111111; Registered Address: 10 Riverside Drive, Suite 402; Contact: Amara Kimani (Cybersecurity Manager)

2. Purpose

This Agreement authorizes the Pentester to conduct controlled, ethical penetration testing and security assessment activities against ParoCyber's systems to identify vulnerabilities, evaluate security controls, and provide remediation guidance.

3. Definitions

Pentest/Assessment: Controlled security testing simulating real-world attack techniques to identify vulnerabilities and assess risk.

Client Assets: Systems, applications, networks, cloud resources, and data owned or managed by the client and explicitly authorized for testing.

Third-Party Assets: Infrastructure or services not owned by the client (e.g., SaaS platforms, hosting providers) that require separate written consent before testing.

Production: Live systems actively serving business operations or customers, where testing must avoid disruption and data integrity issues.

Sensitive Data: Personally Identifiable Information (PII), financial records, authentication secrets, or any regulated information requiring strict handling.

Confidential Information: Non-public business, technical, or security details shared during the engagement, protected under NDA.

Exploit: A technique or action that leverages a vulnerability to gain unauthorized access, escalate privileges, or impact system integrity.

Proof of Concept (PoC): A minimal, controlled demonstration of exploitability without causing harm or violating data handling constraints.

4. Scope of Work (SoW)

In-Scope Assets:

Asset Type	Identifier/URL/IP	Owner	Environment	Notes
Network	External: 203.0.113.0/24; 198.51.100.0/24	Infra	Prod	Fixed outbound IPs allowlisted
Application	https://www.parocyber.example; https://portal.parocyber.example	Product	Prod/UAT	OIDC auth; test accounts provided
API	https://api.parocyber.example/v1	Platform	Prod/UAT	Swagger docs; read-only keys
Cloud (Azure)	Tenant: 00000000-0000-0000-000000000000; Sub: Prod-Infra	Cloud	Prod	Provider approval logged
Cloud (AWS)	Account: 123456789012; Region: af-south-1	Cloud	Prod	Selected services only
Internal	10.20.0.0/16; VLANs: 10.20.10.0/24 (Users), 10.20.20.0/24 (Servers)	IT Ops	Corp	VPN access provided
AD	PAROCYBER.LOCAL; dc1.parocyber. local (10.20.20.10)	IT Ops	Corp	Least-privileged accounts
Wireless	SSID: ParoCyber-Guest; ParoCyber-Corp	IT Ops	Corp	Guest captive portal; Corp WPA2-Enterprise

Out-of-Scope/Prohibited: Unapproved third-party systems; destructive testing (DoS/DDoS); production data exfiltration beyond minimal PoC; unsafe brute force without guardrails; unlawful actions or provider policy violations.

Testing Types: External/Internal Network, Web/Mobile App, API, Cloud, Wireless, Config Review, Social Engineering (approved scenarios).

5. Objectives & Methodology

Objectives: Identify, validate, and prioritize vulnerabilities; assess exploitability and business impact; provide actionable remediation guidance.

Methodology: OWASP Testing Guide, OWASP ASVS/MASVS, NIST SP 800-115, PTES. Techniques include reconnaissance, manual testing, controlled exploitation, configuration review, and targeted automated scanning. Findings will be risk-rated with CVSS v3.1/v4.0 and business impact modifiers.

6. Rules of Engagement (RoE)

Rule	Detail
Authorization	Written authorization signed prior to testing
Testing Window	09–20 Dec 2025, 09:00–18:00 EAT, excluding blackout periods
Source IPs	203.0.113.200–203.0.113.205 (fixed outbound)
Rate Limits	Respect service rate limits; throttle active tests
Emergency Stop	Immediate STOP on adverse impact; notify Client within 15 minutes
Data Handling	Access minimum data; prefer redacted/metadata PoCs
Credentials	Least privilege; unique accounts; encrypted vault storage
Provider Terms	Comply with cloud/SaaS acceptable use; obtain approvals

7. Schedule & Milestones

Milestone	Date/Window	Notes
Kickoff & Access Handover	08 Dec 2025	Comms plan; approvals; accounts provisioned
Testing Window	09–20 Dec 2025 (business hours)	External, internal, app/API, cloud, wireless
Preliminary Readout	15 Dec 2025	High/Critical early disclosure
Draft Report Delivery	22 Dec 2025	Technical & executive summaries
Final Report & Exec Briefing	05 Jan 2026	Board-ready materials
Retest Window	20–25 Jan 2026	Verify remediation of prioritized findings

8. Deliverables

Executive summary, technical report, vulnerability register (CSV/XLS), evidence pack (redacted), retest results, briefings.

9. Legal Authorization & Safe Harbor

Client grants explicit written authorization for activities defined in scope. Safe harbor applies to authorized actions performed with professional care. Third-party consents are Client's responsibility.

10. Fees, Invoicing & Change Control

Item	Detail
Fees	KES 1,250,000 fixed for SoW; Changes at KES 12,000/hour (T&M)
Payment Terms	50% upfront; 50% upon final deliverables; Net-30
Change Control	Written Change Orders approved by both parties
Expenses	Pre-approved travel/lodging billed at cost

11. Confidentiality, Data Protection & Evidence Handling

Mutual NDA; data minimization; redaction of PII/secrets; encrypted storage; 90-day retention then secure destruction; credential vaulting; secure reporting channels; no public disclosure without approval.

12. Operational Safety, Incident Management & Communications

Stability-first testing; Emergency Stop procedure; primary channel (Teams), backup (phone/SMS); daily updates; activity logs retained; high/critical issues opened in Client ticketing.

13. Vulnerability Disclosure & Remediation Windows

Early disclosure for High/Critical within 24 hours. Recommended remediation SLAs: Critical 14 days; High 30 days; Medium 60 days; Low 90 days. Coordinated disclosure only with Client approval.

14. Client Responsibilities

Provide scope and documentation; ensure authorizations; provision access and allowlists; notify stakeholders; maintain backups; attend briefings; facilitate remediation and retesting.

15. Pentester Responsibilities

Adhere to scope and RoE; use vetted tools; protect Client data and secrets; maintain independence; traceable actions; clear, constructive reporting.

16. Liability, Indemnity & Insurance

Aggregate liability capped at total fees paid except for confidentiality/data protection breaches, fraud, willful misconduct, or IP infringement. Mutual indemnity for negligence or breach. Pentester maintains professional liability insurance (certificates available).

17. Compliance & Legal

Comply with applicable computer misuse, data protection, and privacy laws; adhere to sector regulations; respect cloud/SaaS provider testing policies.

18. Intellectual Property

Pentester retains rights to proprietary methodologies and tooling; Client receives perpetual, non-exclusive license to use delivered findings internally and with regulators/auditors under NDA.

19. Term, Termination & Suspension

Agreement is effective through final delivery and retest period. Either party may terminate with 10 business days' notice. Immediate suspension/termination for material breach or emergent operational risk.

20. Force Majeure

No liability for failure or delay due to events beyond reasonable control, with prompt notice and mitigation efforts.

21. Dispute Resolution & Governing Law

Governing Law: Laws of Kenya. Dispute Resolution: negotiation → mediation → arbitration in English, venue agreed by parties, unless urgent injunctive relief is required.

22. General Provisions & Signatures

Entire Agreement; written amendments; assignment restrictions; severability; formal notices via email and registered mail to listed contacts.

Party	Name	Title	Signature	Date
Client (ParoCyber Ltd)	Amara Kimani	Cybersecurity Manager		
Pentester (Contractor)	Bryan M Nturibi	Independent Pentester		

Appendix A – Asset Register (In-Scope)

Asset Type	Identifier/URL/IP	Owner	Environment	Notes
Network	External: 203.0.113.10–.50; Internal: 10.20.0.0/16	Infra	Prod/Corp	Monitoring signatures shared
Application	www.parocyber.example; portal.parocyber.example	Product	Prod/UAT	OIDC scopes: open-id profile email
API	api.parocyber.example/v1	Platform	Prod/UAT	Keys rotated post-engagement
Cloud	Azure Sub: Prod-Infra; AWS: af-south-1	Cloud	Prod	Limited services in scope
AD	PAROCYBER.LOCAL	IT Ops	Corp	LAPS enabled for local admin
Wireless	ParoCyber-Guest; ParoCyber-Corp	IT Ops	Corp	802.1X on Corp; Guest isolated

Appendix B – Change Order Template

CO No.	Requested By	Description of Change	Impact on Scope/Timeline/Fees	Approvals
CO-001	Amara Kimani	Include mobile app testing	Add 3 days: +KES 250,000	Pending

Appendix C – Risk Rating & Remediation Guide

Severity mapping via CVSS v3.1/v4.0 with business impact modifiers (data sensitivity, lateral movement, exploit prevalence). Target remediation SLAs: Critical 14d; High 30d; Medium 60d; Low 90d. Verification via retest evidence and closure criteria.

Appendix D – Communications & Escalation Matrix

Scenario	Response Time	Primary	Backup	Channel
Critical finding	≤ 24h	Amara Kimani	SOC Duty Lead	Secure portal + phone
Service instability	Immediate	NOC Duty Lead	Ops Manager	Phone/SMS + Teams
Daily status	As scheduled	Project Manager	Security Lead	Teams

Appendix E – Tooling & Test Infrastructure

Approved tools: Nmap (7.94), Burp Suite Professional (2025.9), OWASP ZAP (2.15), Nessus (10.x), SQLMap (1.7), Cloudsploit/Azure tooling, Wireshark, PowerShell, Python scripts. Outbound IPs: 203.0.113.200–203.0.113.205. Evidence stored in encrypted vault with 90-day retention.