REDTEAM

RT-ROE-_____-_____ · _____

RULES OF ENGAGEMENT

Offensive Security Engagement

Client: _____ Effective: _____

Window: _____ – _____ Confidential

1 · PURPOSE

These Rules of Engagement ("ROE") govern the conduct of authorized security testing under the accompanying Statement of Work and Authorization Form. They define what may be touched, when, how, and what happens when the unexpected occurs.

2 · PARTIES & AUTHORIZED PERSONNEL

Service provider: REDTEAM — _____, _____.
Client point of contact: _____ · _____ · _____

Client emergency contact: _____ · _____ · _____

3 · AUTHORIZED SCOPE & WINDOW

- Testing is limited to the targets listed in the signed Authorization Form. Nothing else may be scanned, probed, or accessed.
- Active testing window: _____, unless otherwise agreed in writing.
- Passive reconnaissance may run outside the window unless the Client objects.

4 · PERMITTED ACTIVITIES

- Reconnaissance, enumeration, and vulnerability discovery within scope.
- Exploitation and validation up to the tier agreed in the SOW, proof-of-concept only.
- Credential testing using credentials provided by the Client, where agreed.
- Social engineering simulation, only where explicitly agreed in the SOW.

5 · PROHIBITED ACTIVITIES

> **No destruction.** Deleting, corrupting, or destroying data, configurations, or systems is prohibited. Exploitation stops at proof-of-concept.

> **No data exfiltration.** No personal, financial, or production data leaves the environment except minimal evidence artifacts required for the report.

> **No denial of service.** No intentional disruption of availability beyond low-risk, agreed load limits. No action against third-party or shared infrastructure.

> **No scope creep.** Lateral movement is limited to demonstrating the agreed objectives. Any discovery of assets outside scope stops testing of them immediately.

6 · DATA HANDLING (PDPA)

- All data encountered is treated as confidential under the NDA.
- Production data is masked and minimized in all deliverables; only what the evidence requires is retained.
- Evidence and logs are retained for ..... then securely destroyed, or as agreed.

7 · COMMUNICATIONS & ESCALATION

- Critical findings are reported to the Client point of contact within ..... hours of confirmation.
- If testing accidentally impacts availability, the service provider stops immediately and notifies the emergency contact.

- If scope ambiguity arises, testing of the ambiguous target stops until the Client confirms in writing.

8 · INCIDENT HANDLING DURING TESTING

If the Client's monitoring detects the testing activity as suspicious, the Client shall verify with the point of contact before blocking. If a real incident is suspected, the Client may suspend testing; the service provider will assist in distinguishing test activity from the incident.

9 · TERMINATION

Either Party may suspend or terminate the engagement by written notice. Upon termination, testing ceases immediately and evidence is returned or destroyed per the NDA.

10 · AGREEMENT

By signing below, the Parties agree to these Rules of Engagement, the accompanying Statement of Work, Authorization Form, and NDA.

For the Client	For REDTEAM
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

COMPANY STAMP