Rules of Engagement

// PENETRATION TEST — TEMPLATE — RMA SECURITY CONSULTING, LLC

This is a sanitized template provided for evaluation purposes. Actual engagement terms are customized per client and formalized in the Statement of Work.

// 1.0 ENGAGEMENT DETAILS

CLIENT: [Client Legal Name]

ENGAGEMENT TYPE: Internal Network Penetration Test / External / Web App / Cloud / Social Eng.

RMA LEAD: [Engagement Lead Name]

DATE RANGE: [Start Date] through [End Date]

REPORT DELIVERY: Within [X] business days of testing completion

// 2.0 SCOPE DEFINITION

In-Scope Assets

• IP ranges / subnets: [e.g., 10.10.0.0/16]

• Domains: [e.g., *.client.com]

• Cloud tenants: [e.g., Azure tenant ID, AWS account ID]

• Web applications: [e.g., app.client.com, portal.client.com]

• Wireless networks: [if applicable]

Out-of-Scope (Excluded)

• Production databases containing PII/PHI (unless explicitly authorized)

• Third-party hosted services not owned by client

• Physical security testing (unless explicitly authorized)

• Social engineering of specific named individuals (unless authorized)

• [Client to specify additional exclusions]

// 3.0 TESTING PARAMETERS

Testing Windows

Primary testing window: [e.g., Monday–Friday, 8:00 AM – 6:00 PM EST]. After-hours testing: [Authorized / Not Authorized / By prior arrangement only].

Allowed Techniques

✓ Network scanning and enumeration

✓ Vulnerability exploitation (non-destructive)

✓ Credential testing (password spraying with lockout awareness)

✓ Privilege escalation and lateral movement

✓ Data access demonstration (read-only proof, no exfiltration)

✓ Phishing simulation [if social engineering is in scope]

Prohibited Actions

✗ Denial-of-service (DoS/DDoS) attacks

✗ Destructive exploits that could cause data loss

✗ Modification or deletion of production data

✗ Installation of persistent backdoors or implants

✗ Testing against out-of-scope systems

✗ Physical intrusion [unless explicitly authorized]

// 4.0 EMERGENCY STOP PROCEDURE

Either party may halt testing immediately by contacting the designated emergency contacts below. Upon receiving a stop request, RMA will cease all testing activity within 15 minutes and confirm cessation in writing.

ROLE	NAME	PHONE	EMAIL
Client Primary	[Name]	[Phone]	[Email]
Client Backup	[Name]	[Phone]	[Email]
RMA Lead	[Name]	[Phone]	[Email]
RMA Backup	[Name]	[Phone]	[Email]

// 5.0 COMMUNICATION & STATUS

RMA will provide:

• Daily status updates during active testing (brief email or Slack message)

• Immediate notification of any critical/emergency findings

• Draft report for client review before final delivery

• Executive briefing meeting upon report delivery

// 6.0 DATA HANDLING

• **Storage:** All evidence and findings stored on encrypted volumes (AES-256). No data on portable/removable media.

• **Access:** Limited to the RMA engagement lead. No third-party access without written client authorization.

• **Retention:** Engagement data retained for 12 months post-delivery, then securely deleted. Early deletion available on request.

• **Report delivery:** Via encrypted file share with access controls. Not sent as unencrypted email attachments.

// 7.0 AUTHORIZATION

By signing below, both parties acknowledge and agree to the terms of this Rules of Engagement document. This document supplements and is governed by the Master Service Agreement and Statement of Work.

CLIENT **RMA SECURITY**

Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____