

Pentester, LLC

“Know your risks without taking any.”™
hello@pentester.com
www.pentester.com

20238 State Road 7, Suite 108
Boca Raton, Florida, 33498
(337) 821-1337

Parties & Key Details

Customer Legal Name:	
Customer Address:	
Primary Point of Contact (Name / Title):	
POC Email / Phone:	
Billing Contact (Name / Email / Phone):	
Reference SOW (Submission Date & Time):	Submitted 5/19/26, 11:43 AM

1. Engagement Overview & Menu of Services

Customer selects one or more of the following service tracks (each, an "Engagement"). Check all that apply:

- External Penetration Testing

Cost:
- x

Internal Penetration Testing

Cost: ~~\$15,000~~ \$12,000
- x

Red Team Engagement (threat-informed, objective-based, adversary simulation)

Cost: Included
- Social Engineering (Phishing) (opt-in users, consented mail domains, legal safe harbor)

Cost:

Pentester, LLC

"Know your risks without taking any."™

hello@pentester.com

www.pentester.com

20238 State Road 7, Suite 108

Boca Raton, Florida, 33498

(337) 821-1337

- Physical Penetration Testing (pre-authorized facilities only)

Cost:

Approach: Pentester performs expert-led, goal-oriented testing with human analysts; tools are used to accelerate findings, not to check a box. We emulate realistic attacker behaviors, pivot based on evidence, and pursue objectives defined in the SOW, with safety controls and real-time communication.

Duration: Typical project duration is 30–45 days from the agreed start date, subject to Customer readiness, asset access, and timely approvals.

2. Scope & Rules of Engagement (ROE)

2.1 Authorized Systems & People. Testing will target only assets, facilities, accounts, and personnel expressly listed in the SOW and any approved change orders. Customer represents it has the authority to authorize testing on all in-scope items, including cloud and third-party-hosted systems.

2.2 Prohibited Activities (unless explicitly authorized in the SOW):

- [X] Production DDoS/DoS or stress tests; destructive payloads; data corruption; ransomware simulants that could encrypt or lock systems.
- [X] Exfiltration of live sensitive data beyond minimal proof-of-access (use of canary or redacted data preferred).
- [X] Social engineering outside approved targets or outside agreed communication windows.
- [X] Physical entry techniques that risk injury or property damage beyond pre-approved methods.

2.3 Safety & Halt-On-Impact. If material degradation or instability is detected, Pentester may pause testing and notify the POC. Customer designates a 24x7 incident contact and Halt Code below.

2.4 Change Control. Scope or schedule changes require written confirmation (email acceptable) and may affect fees and timeline.

2.5 Lawful Conduct; Safe Harbor. Customer authorizes Pentester to perform testing activities within scope and will ensure applicable providers (e.g., cloud, WAF/CDN, email gateway) are notified or whitelisted as required.

Pentester, LLC

"Know your risks without taking any."™

hello@pentester.com

www.pentester.com

20238 State Road 7, Suite 108

Boca Raton, Florida, 33498

(337) 821-1337

3. Customer Responsibilities

- [X] Provide timely access to network segments, accounts, test data, test MFA methods, badge or escort (for physical), mail configuration (for phishing), and point-of-contact availability.
- [X] Ensure backups, monitoring, and rollback procedures are in place prior to testing.
- [X] Promptly review and approve findings, retest windows, and remediation validations.

4. Deliverables

- [X] Executive Summary (risk narrative, attacker paths, business impact).
- [X] Technical Findings Report (evidence, replication steps, CVSS or priority, remediation guidance).
- [X] Artifacts or Evidence (screenshots, proof-of-access, sanitized payload samples).
- [X] One (1) Retest of verified remediations within 30 days of final report (reasonable effort; out-of-scope changes may require new SOW).

Deliverables are provided in electronic form. Pentester retains ownership of its methods, templates, tools, and know-how; Customer receives a perpetual, non-exclusive license to use the deliverables internally.

5. Fees, Expenses & Payment Terms

5.1 Fees. As specified in section (1) according to each engagement type.

5.2 Payment Schedule. 50% due upon execution (non-cancelable scheduling retainer) and 50% due at project completion (delivery of final readout or report, whichever occurs first). Invoices are net 15 days. Late amounts accrue the lesser of 1.5% per month or the maximum rate permitted by law.

5.3 Expenses & Taxes. Pre-approved travel and reasonable out-of-pocket expenses are billable. Fees exclude taxes; Customer is responsible for applicable taxes, excluding taxes on Pentester's income.

6. Scheduling & Timeline

Pentester, LLC

"Know your risks without taking any."™
hello@pentester.com
www.pentester.com

20238 State Road 7, Suite 108
Boca Raton, Florida, 33498
(337) 821-1337

Pentester will propose a start date upon receipt of the initial 50% payment and required access. Estimated duration is 30–45 days; delays caused by Customer dependencies may extend timeline and incur stand-by fees if materially impacted.

7. Confidentiality & Data Handling

Each party will protect the other's Confidential Information with at least reasonable care. Pentester will: (a) minimize collection of live sensitive data; (b) store evidence securely; (c) retain project data for 90 days after final delivery, then delete it unless longer retention is required by law or expressly agreed.

8. Warranties & Disclaimers

Pentester will perform services in a professional and workmanlike manner consistent with industry standards. Findings are point-in-time and cannot measure or guarantee overall security or future posture. EXCEPT AS EXPRESSLY PROVIDED, SERVICES ARE PROVIDED "AS IS," AND PENTESTER DISCLAIMS ALL OTHER WARRANTIES (INCLUDING MERCHANTABILITY, FITNESS, AND NON-INFRINGEMENT).

9. Indemnification; Limitations of Liability

9.1 Customer Indemnity. Customer will defend, indemnify, and hold harmless Pentester, its affiliates, officers, employees, and contractors from claims, damages, losses, costs, and expenses (including reasonable attorneys' fees) arising from: (i) Customer's systems, data, or third-party claims relating to authorized testing; (ii) Customer's failure to obtain necessary authorizations; or (iii) Customer's misuse of deliverables.

9.2 Pentester Indemnity. Pentester will defend, indemnify, and hold harmless Customer against third-party claims that Pentester's deliverables (as provided) infringe that third party's U.S. intellectual property rights, provided Customer promptly notifies Pentester and allows Pentester sole control of the defense. Pentester may modify or replace deliverables to cure infringement. This does not apply to combinations with non-Pentester items or use outside scope.

9.3 Operational Risk and Limits. Pentester uses commercially reasonable care to avoid outages; however, testing may unintentionally cause slowdowns, alarms, or outages. Customer acknowledges and accepts this risk as inherent to realistic security testing and has implemented backups and rollbacks. TO THE MAXIMUM EXTENT PERMITTED BY LAW, PENTESTER IS NOT LIABLE FOR

Pentester, LLC

"Know your risks without taking any."™

hello@pentester.com

www.pentester.com

20238 State Road 7, Suite 108

Boca Raton, Florida, 33498

(337) 821-1337

INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, COVER, LOST PROFITS, LOSS OF GOODWILL, OR BUSINESS INTERRUPTION DAMAGES. Pentester's aggregate liability under this Agreement shall not exceed the total fees paid or payable for the Engagement giving rise to the claim. These limits do not apply to willful misconduct or gross negligence.

10. Term & Termination

This Agreement begins on the Effective Date and continues through delivery of Services under the SOW. Either party may terminate for material breach not cured within 10 days after written notice. Upon termination, Customer will pay for Services rendered and committed expenses; the initial 50% retainer is applied against work performed and remains non-refundable once scheduling and resourcing occur.

11. Subprocessors & Personnel

Pentester may use qualified employees and vetted subcontractors bound by written confidentiality and data-protection obligations. Upon request, Pentester will provide a certificate of insurance evidencing commercial general liability and professional/technology E&O coverage.

12. Compliance; Backgrounds

Where required by Customer, Pentester will comply with mutually agreed security requirements (e.g., SOC 2, ISO 27001 controls mapping) and provide reasonable evidence. Background checks for on-site testers will be provided upon request where legally permitted.

13. Notices

Notices will be sent to the addresses above (or updated addresses provided in writing). Email is acceptable for day-to-day Engagement communications; legal notices require confirmed receipt.

14. Dispute Resolution; Governing Law

This Agreement is governed by Florida law (conflict-of-law principles excluded). Any dispute arising out of or relating to this Agreement shall be resolved by binding arbitration in Palm Beach County, Florida, under the Commercial Rules of the American Arbitration Association. Either party may seek injunctive or equitable relief in court to protect Confidential Information or IP.

15. Publicity

Pentester, LLC

"Know your risks without taking any."™
hello@pentester.com
www.pentester.com

20238 State Road 7, Suite 108
Boca Raton, Florida, 33498
(337) 821-1337

Pentester may not use Customer's name or logo in marketing without prior written consent, except to identify Customer confidentially to prospective clients under NDA as part of references.

16. Force Majeure

Neither party is liable for delays or failures due to events beyond reasonable control (for example, natural disasters, war, labor actions, or widespread Internet or cloud provider outages), provided the affected party uses reasonable efforts to mitigate.

17. Entire Agreement; Order of Precedence; Assignment

This Agreement (including the SOW and any change orders) is the entire agreement and supersedes prior or contemporaneous proposals and communications about the Engagement. If there is a conflict, the SOW controls for scope, schedule, and fees; otherwise, this Agreement controls. Neither party may assign without the other's consent, except to an affiliate or in connection with a merger, acquisition, or sale of substantially all assets.

18. Counterparts; eSign

This Agreement may be executed in counterparts and by electronic signatures (including DocuSign), each deemed an original and together one instrument.

EXHIBIT A — DATA PROCESSING ADDENDUM (Optional)

Purpose: This DPA applies only if Customer shares Personal Data with Pentester or requires region-specific data handling.

Roles: Customer is the Controller; Pentester is the Processor (or Service Provider under applicable state privacy laws).

Processing Instructions: Pentester will process Personal Data solely to deliver the Services under the Agreement and the SOW, in accordance with Customer's documented instructions.

Security Measures: Pentester maintains administrative, technical, and physical safeguards appropriate to the risk (access control, encryption in transit, secure evidence repositories, least privilege, logging, and retention limits).

Subprocessors: Pentester may use vetted Subprocessors subject to written obligations of confidentiality and data protection; list available upon request. Customer may subscribe to change notifications.

Pentester, LLC

"Know your risks without taking any."™
hello@pentester.com
www.pentester.com

20238 State Road 7, Suite 108
Boca Raton, Florida, 33498
(337) 821-1337

Data Subject Requests: Where applicable, Pentester will reasonably assist Customer in responding to data subject requests received directly relating to Pentester’s processing of Personal Data for the Services.

International Transfers: If cross-border transfers occur, Pentester will use an appropriate transfer mechanism recognized by applicable law.

Return/Deletion: At the end of the Services, Pentester will delete or return Personal Data, unless retention is required by law or expressly agreed.

Audit: Upon reasonable advance notice, Pentester will provide available compliance reports or responses to a security questionnaire no more than annually and subject to confidentiality.

Order of Precedence: In case of conflict between this DPA and the Agreement, this DPA controls for data processing matters.

EXHIBIT B — CONTROL-MAPPING ADDENDUM (SOC 2 / ISO 27001 / NIST CSF)

Purpose: This exhibit maps Pentester’s services and practices to common control frameworks to assist compliance teams. The mappings are illustrative and not a certification.

Service/Practice	SOC 2 (Common Criteria)	ISO/IEC 27001 (Annex A)	NIST CSF (v1.1)
Recon & Attack Surface Management	CC6.1, CC7.2	A.5.12, A.8.16	ID.AM-1, ID.RA-1
Vulnerability Discovery & Validation	CC7.1, CC7.2	A.8.8, A.8.28	PR.IP-12, DE.CM-8

Pentester, LLC

“Know your risks without taking any.”™
hello@pentester.com
www.pentester.com

20238 State Road 7, Suite 108
Boca Raton, Florida, 33498
(337) 821-1337

Exploit Attempt (Controlled)	CC7.3	A.8.32	PR.AC-1, PR.PT-3
Evidence Handling & Retention	CC2.2, CC6.6	A.5.32, A.8.10	PR.DS-1, PR.DS-5
Reporting & Readout	CC2.1	A.6.8	RS.IM-1
Retest & Validation	CC7.3	A.8.29	RS.MI-1
Phishing Simulations	CC6.1	A.6.1, A.6.10	PR.AT-1, PR.PT-1
Physical Testing	CC6.1	A.7.4, A.7.5	PR.AC-2, PR.PT-3

Note: Framework references are approximate and provided to facilitate internal mapping; they do not imply certification or auditor attestation.

Pentester, LLC

“Know your risks without taking any.”™
hello@pentester.com
www.pentester.com

20238 State Road 7, Suite 108
Boca Raton, Florida, 33498
(337) 821-1337

Signature Page
Customer

By:

Name:

Title:

Date:

Pentester, LLC

By:

Name:

Sara Broderius

Date:
