

Penetration Testing (VAPT) - Schedule PROF-1

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary

Service Provider shall facilitate Penetration Testing and Vulnerability Assessment services (“VAPT Services”) on behalf of Client. These services are intended to evaluate the security posture of Client systems by simulating attacks and identifying vulnerabilities. Service Provider does not perform penetration testing directly; all testing is conducted by qualified third-party providers. Service Provider provides coordination, preparation, and facilitation of testing activities but does not guarantee outcomes or remediation.

Scope of Services

- Scoping discussions with Client to define objectives, systems in-scope, and testing methodologies (e.g., external, internal, web application, wireless).
- Coordination with independent penetration testing firms to develop a Statement of Work.
- Facilitation of contracts between Client and testing provider; Service Provider may act as reseller for administrative convenience.
- Preparation activities, including evidence gathering, system access provisioning, and test scheduling.
- Delivery of testing results and reports from the third-party provider to Client stakeholders.
- Advisory assistance with prioritizing remediation steps following test completion.

Exclusions

- Service Provider is not a penetration testing provider and does not conduct tests directly.
- Responsibility for test results, methodologies, or findings lies solely with the engaged third-party provider.
- Any guarantee of security, compliance, or remediation following testing.
- Remediation of vulnerabilities identified during testing, which must be scoped separately as projects.
- Coverage of systems not expressly defined as in-scope in the agreed Statement of Work.
- Liability for operational disruption or downtime resulting from authorized testing activities.

Client Responsibilities

- Approve systems, applications, and environments to be tested.
- Provide accurate scoping information and timely system access required for testing.
- Obtain any required permissions from hosting providers, cloud platforms, or third parties for testing activities.
- Review and act upon findings, including implementing remediation steps.
- Retain ultimate responsibility for system security, compliance, and risk management.

General Terms

- VAPT Services are facilitation-only; Service Provider is not responsible for conducting or certifying penetration testing results.
- If Service Provider resells testing services, Client understands that the third-party provider is solely responsible for testing activities, reports, and findings.
- Testing inherently carries risk of service disruption, performance degradation, or false positives. Client accepts these risks as part of the engagement.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Where Service Provider acts as reseller, third-party testing fees are passed through to Client in addition to Service Provider’s facilitation fees.
- Service Provider disclaims liability for regulatory fines, penalties, or damages arising from penetration testing results or unremediated vulnerabilities.