VAPT request for proposal template

BERRY9 IT SERVICES
VAPT services, Hyderabad
berry9.com

Copy this into your own document and fill in the blanks. Send the same completed document to every vendor, so that the quotes can be compared. Delete the grey hints before you send it.

1. Purpose

We are asking for vulnerability assessment and Penetration Testing because:

_____.

Launch, customer request, audit, regulator, a recent change or an incident.

2. Scope

System	Address or version	Type	Roles	Environment

Out of scope: _____.

3. Test approach

- ☐ Black box, gray box or white box: _____.
- ☐ External, internal or both: _____.
- ☐ Manual testing by engineers is required, and the vendor states what is done by tools and what by hand.
- ☐ The vendor names the methods and lists it follows, such as OWASP Top 10, OWASP API Security Top 10 or OWASP MASVS.

4. Environment and rules of engagement

- ☐ Testing is done on staging / production (circle one), in these hours: _____.
- ☐ We will provide test accounts, a named contact and a notice to our hosting provider.
- ☐ The vendor describes how it will avoid disruption and what it will do if it finds something critical.

5. Compliance requirements

- ☐ The test must satisfy: _____.
- ☐ The auditor must be CERT-In empanelled: yes / no / to be confirmed.
- ☐ The vendor states clearly whether it meets this requirement.

6. Deliverables

- ☐ A report for management and a technical report for engineers.
- ☐ For each finding: a rating and how it was rated, evidence, steps to reproduce and a fix.
- ☐ A walkthrough call, and a retest of fixed findings within ____ days. The vendor states the retest terms and any charge.
- ☐ A sample report from a previous engagement, with the client's details removed.

7. Timeline

Start date: _____ Draft report due: _____ Retest window: _____.

8. Team and experience

- ☐ Names and roles of the people who will test, and their relevant experience.
- ☐ Whether any work is done by subcontractors.
- ☐ The vendor's contact during the test.

9. Confidentiality and data

- ☐ Where findings and credentials are stored, who may see them, and when they are deleted.
- ☐ A confidentiality agreement is signed before work starts.

10. Price and terms

- ☐ A fixed price for the scope above, with GST shown separately, and a list of what is not included.
- ☐ How changes to the scope are priced, and the payment terms.

11. How replies will be judged

Replies are scored on the attached scorecard. Any must-have in sections 5 and 6 is a pass or fail item. Please send your reply by _____ to _____.