Standard Security Questionnaire

1. Do you have an Information Security Policy in place?

2. Is your organization ISO 27001 certified?

3. Do you conduct regular penetration tests?

4. Do you have a formal risk assessment process?

5. Are employees required to complete annual security training?

6. Do you enforce multi-factor authentication for all users?

7. Is sensitive data encrypted at rest?

8. Is sensitive data encrypted in transit?

9. Do you maintain audit logs of all system activity?

10. Are backups performed regularly and tested?

11. Do you have an incident response plan?

12. Has the incident response plan been tested in the last year?

13. Do you have a business continuity plan?

14. Is physical access to data centers restricted and logged?

15. Do you use a secure software development lifecycle (SDLC)?

16. Are code changes peer-reviewed before deployment?

17. Is third-party software scanned for vulnerabilities?

18. Do you patch operating systems and applications promptly?

19. Are endpoints protected with anti-malware software?

20. Do you monitor for unauthorized access attempts?

21. Are default passwords changed before use?

22. Is there a formal process for granting and revoking user access?

23. Do you maintain an inventory of IT assets?

24. Are systems configured according to security baselines?

25. Are network devices hardened before deployment?

26. Do you segment networks to limit access to sensitive data?

27. Is data disposal handled securely (e.g., disk wiping)?

28. Do you have a DLP (Data Loss Prevention) solution in place?

29. Are vendor risk assessments conducted regularly?

30. Is cloud infrastructure managed securely and monitored?

31. Do you have a secure email gateway to filter threats?

32. Are email communications encrypted when necessary?

33. Is access to production data limited to authorized personnel?

34. Do you conduct internal security audits?

35. Are mobile devices encrypted and remotely wipeable?

36. Do you track and manage vulnerabilities through remediation?

37. Are users educated about phishing attacks?

38. Do you conduct background checks on employees with access to sensitive data?

39. Is there a process for reporting security incidents internally?

40. Are service accounts monitored and reviewed?

41. Are administrative privileges granted based on least privilege?

42. Do you enforce session timeouts and auto-logout policies?

43. Are system clocks synchronized using a trusted time source?

44. Are wireless networks secured using strong encryption protocols?

45. Are third-party integrations reviewed for security risks?

46. Is customer data segregated in multi-tenant environments?

47. Do you monitor data egress points?

48. Is there a policy for acceptable use of IT resources?

49. Are source code repositories access-controlled?

50. Do you track regulatory compliance (e.g., GDPR, HIPAA)?