50 Security Questions AI/SaaS Founders Should Prepare For

Buyer questions on security, privacy, AI use and procurement readiness · for early B2B conversations, security questionnaires and trust-material preparation.

Purpose: This checklist helps AI/SaaS founders identify common buyer questions before a procurement, privacy or security review becomes urgent. It is professional orientation, not legal advice, certification, audit, penetration test or buyer approval guarantee.

Security governance

1. Who is responsible for information security in your product and company?
2. How are security-relevant decisions documented and reviewed?
3. How do you track security gaps, exceptions and remediation actions?
4. Which policies or internal rules define acceptable use, access and handling of customer data?
5. How do you prevent security statements from becoming stronger than your actual evidence?

Data protection and processing

6. Which personal data and customer content are processed by the product?
7. Where is data hosted, processed and backed up?
8. Which subprocessors or providers may process customer data?
9. How can customers request deletion, export or correction of data?
10. Which retention periods are defined for customer data, logs and backups?

AI use and model/provider handling

11. Which AI or LLM providers are used in the product or operations?
12. What data is sent to AI providers, and under which configuration?
13. Is customer data used for model training, and how can this be evidenced?
14. Are prompts, outputs or intermediate results logged? If yes, where and for how long?
15. How do you explain AI usage to buyers without overclaiming safety, privacy or compliance?

Access, roles and operations

16. Who has administrative access to production systems?
17. Is MFA enforced for cloud, repository, payment, AI-provider and admin accounts?
18. How are joiner/mover/leaver processes handled for employees, freelancers and agencies?
19. How often are privileged accesses reviewed?
20. How is support access to customer data restricted and logged?

Technical baseline

21. How are production, test and development environments separated?
22. How are secrets, API keys, certificates and tokens stored and rotated?
23. Which public endpoints exist, and how are they protected?
24. Who is responsible for patching dependencies, infrastructure and managed services?
25. How are backups, restore tests, monitoring and alerts handled?

Evidence and buyer communication

26. Which statements can be supported by documents, provider evidence or internal records?
27. Which open gaps should be communicated transparently rather than hidden?
28. Which evidence can be shared externally, and what must be redacted or NDA-bound?
29. How do you assemble responses before sending them to a buyer?
30. Who approves external security, privacy and AI-use statements before submission?

Trust material and next steps

31. Do you have a concise trust or security overview for buyer conversations?
32. Do you maintain a current subprocessor overview?
33. Do you have a 30/60/90-day action plan for known gaps?
34. Which buyer questions are likely to block a deal if not prepared?
35. When should you use a template pack, a review, or a focused readiness sprint instead of answering alone?

Next step: If a buyer has already sent a security questionnaire, do not answer from memory. First separate evidenced statements, open gaps, assumptions and answers that require internal or external review.

Preferred contact: info@a-r-c.me
Website: www.a-r-c.me
Offer: A-R-C AI/SaaS Security & Trust Readiness