

Vendor Security Questionnaire

Questions to ask before handing a SaaS vendor your data.

Data Handling

1. What data of ours will you store, and where is it physically hosted?
2. Is our data encrypted, both in transit and at rest?
3. Do you sell, share, or use our data for anything beyond providing the service?

Access & Authentication

1. Do you support two-factor authentication?
2. Do you support single sign-on if we need it?
3. How is access to our data controlled and logged on your end?

Compliance & Certifications

1. Do you hold any relevant security certifications (SOC 2, ISO 27001, etc.)?
2. Are you compliant with relevant regulations for our industry?

Incident Response

1. What's your process if you experience a data breach?
2. How quickly, and how, would you notify us if our data was affected?

Business Continuity

1. What happens to our data if you go out of business or discontinue the product?
2. Can we export our data at any time, in a usable format?
3. What's your uptime track record, and do you have a status page?

Subprocessors

1. Do you use third-party subprocessors, and who are they?
2. Are we notified if that list changes?

Before Signing

- ☐ Answers reviewed against how sensitive the data actually is
- ☐ Red flags taken seriously, not brushed past
- ☐ Contract terms match what was represented in the questionnaire