FREE RESOURCE / XBITIUM SECURITY

Vendor Security Questionnaire

Vet your suppliers — and rehearse for the day a client vets you.

This document works two ways. Send it **to** a supplier before you trust them with your data. And read it as the questions your **own** biggest clients will eventually send you — because vendor security questionnaires are now a routine part of winning business, and the deal stalls until you can answer them. If these questions make you nervous about your own answers, that nervousness is precisely why this document exists.

THE PART NOBODY WARNS SMALL BUSINESSES ABOUT

The fastest-growing reason small companies lose deals is not price or product — it is failing a security questionnaire sent by a larger client's procurement team. The good news: the questions are predictable. Prepare your answers once, and you stop losing those deals.

1. Access and authentication

Question	Yes	No	Notes / evidence
Is multi-factor authentication enforced on all administrative and remote access?			
Are user accounts unique to individuals (no shared logins)?			
Is access removed promptly when staff leave or change roles?			
Is the principle of least privilege applied to data access?			

2. Data protection

Question	Yes	No	Notes / evidence
Is data encrypted in transit (e.g. TLS) and at rest?			
Do you know where our data would be stored (which country or region)?			
Is our data logically separated from other customers' data?			
What is your data retention and secure deletion policy?			

3. Operations and patching

Question	Yes	No	Notes / evidence
Are systems patched on a defined schedule?			
Do you run regular vulnerability scans or penetration tests?			
Is there endpoint protection on systems that handle our data?			
Are backups performed, encrypted, and tested?			

4. Incident response

Question	Yes	No	Notes / evidence
Do you have a documented incident response plan?			
Will you notify us of a breach affecting our data, and how quickly?			
Have you had a security incident in the last 24 months?			
Do you carry cyber liability insurance?			

5. Governance and compliance

Question	Yes	No	Notes / evidence
Do you have written information security policies?			
Do you hold any certifications (SOC 2, ISO 27001, and so on)?			
Do staff receive regular security awareness training?			
Do you assess the security of your own subcontractors?			

Scoring guidance

There is no universal pass mark — weight the answers by how much access the vendor has to your sensitive data. A marketing tool that never touches customer records warrants less scrutiny than a payroll processor.

Focus on the **No** answers in access, data protection, and incident response; that is where a weak vendor becomes your breach.

USING THIS ON YOURSELF

Fill this in as though a client had sent it to you. Every 'No' is either a gap to close or an answer to prepare. Do that before the questionnaire arrives, and you turn a deal-stalling scramble into a same-day reply. That difference wins contracts.

WHEN YOU WANT TO KNOW WHAT IS ACTUALLY EXPOSED

A checklist tells you what *should* be true. A scan tells you what *is* true. Xbitium will scan your public-facing systems and send you a real report in 48 hours — free, nothing to install, no obligation. If you are in good shape, we will say so and leave you alone.

Request your free external scan at xbitiumsecurity.com