

Vendor Security Questionnaire — Template

SecureBusinessHub — Educational Resource for SMBs

Section A — Company & Compliance

- Legal entity name, headquarters and EU representative (if applicable).
- List current certifications: ISO 27001, SOC 2 Type II, PCI-DSS, ENS.
- Date of most recent independent security audit and summary of findings.
- Named Data Protection Officer and contact email.

Section B — Data Handling

- What categories of our data will you process?
- In which countries / cloud regions is data stored and backed up?
- Sub-processors used and how customers are notified of changes.
- Data retention periods and deletion procedures upon contract termination.

Section C — Access Control

- Is multi-factor authentication enforced for all employee and admin accounts?
- How is privileged access managed, logged and reviewed?
- Joiner / mover / leaver process and maximum off-boarding time.

Section D — Application & Infrastructure Security

- Frequency of vulnerability scanning and independent penetration testing.
- Secure development lifecycle: code review, SAST, DAST, dependency scanning.
- Encryption in transit (TLS version) and at rest (algorithm and key management).

Section E — Incident Response

- Do you have a documented incident response plan? Date last tested?
- Notification SLA to customers when a security incident is confirmed.
- Cyber insurance coverage and limit.

Section F — Business Continuity

- RTO and RPO commitments for the service we will consume.
- Date of most recent disaster-recovery test and outcome.

Section G — Attachments

- Latest SOC 2 / ISO 27001 report (under NDA).
- Information security policy summary.
- Standard Data Processing Agreement (DPA).

This template is provided for educational purposes. Adapt to your organisation's context and seek professional advice where appropriate.