

[Company name]

Vendor Security Questionnaire

Sent by	[Company name]
Sent to	[Vendor name]
Reply by	[Reply by]
Questions	68 in 7 sections
Questions to	[Security contact]

1. Instructions for the vendor

[Company name] uses this questionnaire to assess the security of vendors that hold or reach its customer data, or that its production service depends on. Answer each question Yes, No or Partial, add a short comment, and attach or link the evidence requested. Answer Not applicable only with a reason.

If you have a current SOC 2 Type 2 report covering the service [Company name] buys, send it first. [Company name] will review the report and may then ask only the questions it does not answer.

Return the completed questionnaire by [Reply by] to [Security contact]. Evidence may be redacted, and anything marked confidential is handled under the confidentiality terms between the two companies.

2. Company and compliance posture

ID	Question	Evidence requested	Criterion	Answer
A1	Does your company have a current SOC 2 Type 2 report?	The report under a confidentiality agreement, or its opinion and scope pages	CC9.2, tests the whole control set	
A2	If not, do you have a SOC 2 Type 1 report, an ISO 27001 certificate or another independent attestation?	The report or certificate, with its scope	CC9.2, tests the whole control set	
A3	Is a named person accountable for your security program?	Name and title	CC9.2, tests CC1.3 structure and reporting	

ID	Question	Evidence requested	Criterion	Answer
A4	Are your security policies written, approved by management and reviewed at least once a year?	List of policies with approval dates	CC9.2, tests CC5.3 policies and procedures	
A5	Do employees and contractors acknowledge a code of conduct and the security policies?	Acknowledgment record	CC9.2, tests CC1.1 integrity and ethics	
A6	Are background checks performed, where law allows, on staff with access to customer data?	Policy excerpt	CC9.2, tests CC1.4 hiring and competence	
A7	Do all staff complete security awareness training at hire and every year?	Training completion report	CC9.2, tests CC1.4 hiring and competence	
A8	Do you perform a formal risk assessment at least once a year?	Summary of the latest assessment	CC9.2, tests CC3.1 to CC3.4 risk assessment	
A9	Do you carry cyber liability insurance?	Certificate of insurance	CC9.2, tests CC9.1 disruption risk	

3. Access control

ID	Question	Evidence requested	Criterion	Answer
B1	Is single sign-on used for staff access to internal and production systems?	Identity provider application list	CC9.2, tests CC6.1 logical access	
B2	Is multi-factor authentication enforced for all staff accounts?	Identity provider enforcement setting	CC9.2, tests CC6.1 logical access	
B3	Is multi-factor authentication enforced for administrator and cloud console access?	Cloud console sign-in policy	CC9.2, tests CC6.1 logical access	
B4	Is access to production limited by role to the people who need it?	Production roles with their member counts	CC9.2, tests CC6.3 least privilege	
B5	Is production access approved by a manager before it is granted?	One approved access request	CC9.2, tests CC6.2 user provisioning	
B6	Is access to production reviewed at least every quarter?	Most recent access review	CC9.2, tests CC6.2 and CC6.3 access reviews	

ID	Question	Evidence requested	Criterion	Answer
B7	Is access removed within one business day of a person leaving?	One offboarding record	CC9.2, tests CC6.2 user provisioning	
B8	Are shared and generic accounts prohibited, or controlled and logged where they cannot be avoided?	Policy excerpt	CC9.2, tests CC6.1 logical access	
B9	Do password rules set a minimum length and block known breached passwords?	Password settings	CC9.2, tests CC6.1 logical access	
B10	Can our users sign in to your product with single sign-on or multi-factor authentication?	Product documentation	CC9.2, tests CC6.1 logical access	
B11	Can your staff reach our data only through approved tools that log each access?	Description of support access	CC9.2, tests CC6.1 logical access	

4. Data protection and encryption

ID	Question	Evidence requested	Criterion	Answer
C1	Is our data encrypted at rest with AES-256 or an equivalent standard?	Storage encryption settings	CC9.2, tests CC6.1 logical access	
C2	Is all data in transit over public networks encrypted with TLS 1.2 or higher?	TLS scan result	CC9.2, tests CC6.7 data in transit	
C3	Are encryption keys held in a key management service with access restricted and logged?	Key policy screenshot	CC9.2, tests CC6.1 logical access	
C4	Is our data logically separated from other customers' data?	Architecture description	CC9.2, tests CC6.1 logical access	
C5	Is production customer data kept out of development and test environments?	Policy excerpt or data flow	CC9.2, tests CC6.1 and CC8.1	
C6	Do you classify data and apply handling rules by classification?	Data classification standard	CC9.2, tests CC6.1 logical access	
C7	Is our data deleted or returned within a set period after the contract ends?	Retention schedule and deletion procedure	CC9.2, tests CC6.5 data disposal	
C8	Are backups encrypted and stored separately from production?	Backup configuration	CC9.2, tests CC6.1 and A1.2	

ID	Question	Evidence requested	Criterion	Answer
C9	Are secrets such as API keys kept in a secrets manager and out of source code?	Secrets manager and secret scanning settings	CC9.2, tests CC6.1 logical access	
C10	Are company laptops encrypted and managed by a device management tool?	Device compliance report	CC9.2, tests CC6.8 malware prevention	
C11	Do company laptops run endpoint protection that is kept up to date?	Endpoint protection coverage report	CC9.2, tests CC6.8 malware prevention	

5. Infrastructure and network

ID	Question	Evidence requested	Criterion	Answer
D1	Is production hosted with a cloud provider whose own SOC 2 report you review every year?	Provider name and last review	CC9.2, tests CC9.2 vendor risk	
D2	Is network access to production restricted by rules that deny by default?	Security group or firewall rule summary	CC9.2, tests CC6.6 network boundaries	
D3	Is a web application firewall or equivalent in front of public endpoints?	Configuration screenshot	CC9.2, tests CC6.6 network boundaries	
D4	Are production systems built from a documented hardening baseline or infrastructure code?	Baseline document or code reference	CC9.2, tests CC7.1 vulnerability monitoring	
D5	Do you scan infrastructure and dependencies for vulnerabilities at least monthly?	Most recent scan summary	CC9.2, tests CC7.1 vulnerability monitoring	
D6	Are critical vulnerabilities fixed within a written deadline of 30 days or less?	Remediation policy and tracker excerpt	CC9.2, tests CC7.1 vulnerability monitoring	
D7	Has a penetration test covering the service been performed in the last 12 months?	Executive summary or attestation letter	CC9.2, tests CC4.1 and CC7.1	
D8	Are application and infrastructure logs collected centrally and kept for a set retention period?	Logging configuration and retention setting	CC9.2, tests CC7.2 anomaly monitoring	
D9	Are alerts configured for security events, with a named person to respond?	Alert rules and on call schedule	CC9.2, tests CC7.2 anomaly monitoring	

ID	Question	Evidence requested	Criterion	Answer
D10	Are logs protected from change or deletion by the people whose actions they record?	Log access settings	CC9.2, tests CC7.2 anomaly monitoring	

6. Secure development

ID	Question	Evidence requested	Criterion	Answer
E1	Is every change to production tracked in a ticket or pull request?	One example change	CC9.2, tests CC8.1 change management	
E2	Is code reviewed and approved by someone other than the author before it is merged?	Branch protection settings	CC9.2, tests CC8.1 change management	
E3	Do automated tests and security checks run before each deployment?	Pipeline configuration	CC9.2, tests CC8.1 change management	
E4	Are development, test and production environments separated?	Environment diagram	CC9.2, tests CC8.1 change management	
E5	Do you scan code and dependencies for known vulnerabilities and committed secrets?	Scanner settings	CC9.2, tests CC7.1 and CC8.1	
E6	Is there a documented emergency change procedure, with review after the fact?	Procedure	CC9.2, tests CC8.1 change management	
E7	Do developers receive secure coding training?	Training record	CC9.2, tests CC1.4 hiring and competence	
E8	Can a deployment be rolled back to the last working release?	Rollback procedure	CC9.2, tests CC8.1 change management	

7. Incident response and business continuity

ID	Question	Evidence requested	Criterion	Answer
F1	Do you have a written incident response plan approved by management?	Plan table of contents	CC9.2, tests CC7.3 and CC7.4 incidents	

ID	Question	Evidence requested	Criterion	Answer
F2	Is the incident response plan exercised at least once a year?	Most recent exercise record	CC9.2, tests CC7.4 incident response	
F3	Will you notify us of a security incident affecting our data within a contracted time?	Contract clause or policy, with the time	CC9.2, tests CC7.4 incident response	
F4	Do you perform a root cause analysis after significant incidents?	One redacted example	CC9.2, tests CC7.5 incident recovery	
F5	Is our data backed up at least daily?	Backup configuration	CC9.2, tests CC7.5 and A1.2	
F6	Are restores from backup tested at least once a year?	Most recent restore test	CC9.2, tests CC7.5 and A1.3	
F7	Do you have a business continuity and disaster recovery plan with recovery time and recovery point objectives?	Plan excerpt with the objectives	CC9.2, tests CC9.1 disruption risk	
F8	Is the disaster recovery plan tested at least once a year?	Test summary	CC9.2, tests CC9.1 and A1.3	
F9	Do you publish a status page or otherwise notify customers of outages?	Status page address	CC9.2, tests CC2.3 external communication	
F10	Do you commit to an uptime target in your contracts?	Service level terms	CC9.2, tests A1.1 capacity	

8. Subprocessors and privacy

ID	Question	Evidence requested	Criterion	Answer
G1	Do you publish a list of the subprocessors that handle customer data?	List or its address	CC9.2, tests CC9.2 vendor risk	
G2	Will you notify us before adding a new subprocessor?	Contract clause	CC9.2, tests CC9.2 vendor risk	
G3	Do you review the security of each subprocessor before use and every year?	One vendor review record	CC9.2, tests CC9.2 vendor risk	
G4	Do your subprocessor contracts carry security and confidentiality terms at least as strict as ours?	Template clause	CC9.2, tests CC9.2 vendor risk	

ID	Question	Evidence requested	Criterion	Answer
G5	Will you sign a data processing agreement?	Data processing agreement	CC9.2, tests CC9.2 vendor risk	
G6	Do you collect only the personal data needed to provide the service?	Data inventory	CC9.2, tests privacy commitments	
G7	Do you handle requests to access, correct or delete personal data within the legal deadlines?	Procedure	CC9.2, tests privacy commitments	
G8	Is our data kept out of model training and away from third parties other than the listed subprocessors?	Policy or contract term	CC9.2, tests privacy commitments	
G9	Do you tell customers which controls they are responsible for (complementary user entity controls)?	List of customer responsibilities	CC9.2, tests CC2.3 external communication	

9. Vendor attestation

The answers above are accurate to the best of the signer's knowledge on the date signed. [Vendor name] will tell [Company name] if a material answer stops being true during the contract.

Signing for the vendor

Name:

Signature:

Date:

10. Scoring the answers

For the reviewer at the company that sent the questionnaire. Delete this section and the next one before sending.

Answer	Points	Meaning
Yes	2 points	The control is in place and the evidence shows it.
Partial	1 point	In place for part of the scope, or started but not yet operating for long.
No	0 points	Not in place.

Answer	Points	Meaning
Not applicable	Left out	The question does not apply to the service. The reviewer agrees in a note, and it leaves both the score and the maximum.

Each question carries a weight from 1 to 3, and its score is the points times the weight. Weight 3 marks a critical question: multi-factor authentication, production access, offboarding, encryption, vulnerability deadlines, code review, the incident response plan, breach notice and the SOC 2 report itself. Add the weighted scores by section and in total, and compare the total with the maximum.

Result	Decision
85% or more, and no critical question answered No	Approve. Record the review date and set the next one.
70% to 84%, and no critical question answered No	Approve with follow-ups, each with an owner and a date in the vendor register.
Below 70%, or any critical question answered No	The security owner decides: decline, accept the risk in writing, or require a fix before signing.

The thresholds are a starting point, not a standard. Write the rule you use into your vendor management policy and apply it the same way to every vendor of the same tier.

11. Worked example: Lanternfish

Moonrake, a fictional company of about ten people selling API security monitoring to fintech companies, sends usage events from its product to Lanternfish, a fictional analytics provider. Lanternfish has a SOC 2 Type 1 report and is in its first Type 2 observation period, so Moonrake sent the full questionnaire.

Section	Questions	Weighted score	Maximum	Percent
Company and compliance posture	9	27	30	90%
Access control	11	46	48	96%
Data protection and encryption	11	46	46	100%
Infrastructure and network	10	34	36	94%
Secure development	8	28	28	100%
Incident response and business continuity	10	30	38	79%
Subprocessors and privacy	9	30	30	100%

Section	Questions	Weighted score	Maximum	Percent
Total	68	241	256	94%

Lanternfish scored 94% in total with no critical question answered No, so the rule says approve. Moonrake approved, and turned every answer that was not a plain Yes into a note or a follow-up:

ID	Answer	Lanternfish comment	Reviewer note
A1	Partial	Type 1 report issued. Type 2 observation period running, report expected next quarter.	Accept the Type 1 now. Ask for the Type 2 when it is issued.
B6	Partial	Quarterly review for the AWS production account started two months ago. Other systems are reviewed once a year.	Follow up: confirm the second quarterly review happened.
D7	Partial	The web application was tested. The ingestion API was not in scope.	Follow up: ask for the ingestion API to be in the next test, since our events reach it.
F2	No	Plan approved, no exercise run yet. A tabletop is scheduled.	Follow up: ask for the tabletop record within 90 days.
F8	Partial	Database restores are tested every quarter. A full recovery test has not been run.	Follow up: full recovery test before renewal.
F10	No	No uptime commitment in the standard contract.	Accepted: Lanternfish is not on our customer facing path.

Moonrake recorded the approval, each follow-up with an owner, and the next review in its vendor register. The full answer set is on the Lanternfish sheet of the Excel version.

12. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Security contact]	The role and email address a reader writes to with questions.
[Vendor name]	The vendor the questionnaire or report review is about, by its legal name.
[Reply by]	The day the answers are due, for example two weeks after sending.

Source

Source: free template from www.polaralabs.com/templates/vendor-security-questionnaire (CC BY 4.0).