

Vendor Security Questionnaire

A short, usable questionnaire for assessing a vendor before they touch your data. Each question says what a good answer looks like and what should worry you. Use it in the other direction too: these are the questions your own customers' security teams will ask you.

Updated September 2026. 31 questions. A fillable Excel sheet with scoring and a Word copy are at traztech.ca/templates. Send sections 1 to 4 to every vendor; add sections 5 to 8 for vendors that store or process customer or personal data.

How to use it

Tier your vendors first. A vendor with access to production or customer personal information is high risk and gets the full questionnaire plus their assurance report. A tool that holds no sensitive data may need only section 1.

Ask for evidence, not just answers. A current SOC 2 Type 2 report or ISO 27001 certificate answers most of these questions. Read the report's scope, its exceptions and its "complementary user entity controls", the controls the vendor expects you to run.

Long industry questionnaires. Buyers may send you the SIG (Shared Assessments), the CAIQ (Cloud Security Alliance) or the HECVAT (higher education). This questionnaire covers the same core topics in a size a small company can answer and review.

Why it matters in Canada. Under PIPEDA you remain accountable for personal information you transfer to a vendor for processing, and must protect it by contract. Under Quebec Law 25, you must assess privacy impacts before personal information leaves Quebec.

Vendor: _____ Reviewed by: _____

Data the vendor will access: _____ Risk tier: _____

1. Company and assurance

Question	A good answer	Red flag
1.1 Do you have a current SOC 2 Type 2 report or ISO 27001 certificate? Please share it.	Report dated within the last 12 months, scope covers the service you are buying.	Only a Type 1 from years ago; scope excludes the product; "we are working on it" with no date.
1.2 Who is responsible for security, and to whom do they report?	A named person with the authority and time to act.	Nobody named, or "our cloud provider handles security".
1.3 When was your last independent penetration test, and were the findings fixed?	Within 12 months, with a summary or attestation letter and remediation status.	Never tested, or findings still open with no plan.
1.4 Do you carry cyber insurance?	Yes, with limits appropriate to the data they hold.	No coverage for a vendor holding sensitive data.
1.5 Have you had a security incident affecting customer data in the last 3 years?	A candid answer, with what changed afterwards.	Evasion, or "no" contradicted by public reporting.

2. Access control

Question	A good answer	Red flag
2.1 Is MFA enforced for all staff and for admin access to production?	Yes, enforced, not optional.	MFA "available" but not required.
2.2 How many staff can access our data, and how is that access approved and reviewed?	A small, named group; approval and quarterly reviews.	"All engineers" or no reviews.
2.3 How quickly is access removed when someone leaves?	Same day or within 24 hours, tied to HR.	No defined timeline.
2.4 Do you support SSO and MFA for our users of your product?	SAML or OIDC SSO, enforced MFA, role-based access.	Passwords only, or SSO behind the most expensive plan with no alternative.

3. Infrastructure and operations

Question	A good answer	Red flag
3.1 Where is our data hosted, and in which regions?	Named provider and regions; Canadian hosting if you need it.	"Various locations" with no list.
3.2 Is data encrypted in transit and at rest? Who manages the keys?	TLS 1.2 or higher, AES-256 at rest, keys in a managed KMS with limited access.	Encryption at rest "planned".
3.3 How do you find and fix vulnerabilities, and how fast?	Regular scanning, defined remediation times by severity.	No scanning, or no timelines.
3.4 How are code and infrastructure changes reviewed before production?	Peer review, automated tests, restricted deploy rights.	Developers push straight to production.
3.5 What do you log, and for how long?	Security-relevant events centralised and kept 12 months or more.	Logs kept days, or not reviewed.

4. Incident response and continuity

Question	A good answer	Red flag
4.1 Do you have a tested incident response plan?	Yes, tested in the last year.	No plan, or never tested.
4.2 How quickly will you notify us of an incident affecting our data?	A contractual commitment, commonly 24 to 72 hours from confirmation.	"As required by law" only, with no timeline.
4.3 What are your recovery time and recovery point objectives?	Stated targets, tested restores.	No targets, backups never restored.
4.4 What is your uptime commitment and history?	An SLA and a public status page.	No SLA for a critical service.

5. Data handling and privacy

Question	A good answer	Red flag
5.1 What personal information will you process, and for what purposes?	Specific and limited to the service.	Use of our data to train models or for marketing without consent.
5.2 Will you sign a data processing agreement?	Yes, covering purpose, security, subprocessors, breach notice, deletion and audit rights.	Refusal, or terms that let them change use unilaterally.
5.3 Who are your subprocessors and where are they?	A published list with advance notice of changes.	No list.
5.4 How do you delete our data at the end of the contract?	Deletion within a stated period, with confirmation on request.	Data kept indefinitely.
5.5 Can you support access and deletion requests from individuals?	A documented process with response times.	No process.

6. Application security

Question	A good answer	Red flag
6.1 Do you follow a secure development process?	Code review, dependency scanning, secrets management, security testing before release.	No review or scanning.
6.2 How do you separate customers' data from each other?	Tenant isolation described and tested.	"It's handled by the database" with no detail.
6.3 Do you run a vulnerability disclosure program?	A published way to report issues.	No way to report.

7. People

Question	A good answer	Red flag
7.1 Are staff background-checked, where lawful, and trained on security?	Yes, at hire and annually for training.	No training.
7.2 Do contractors with access follow the same rules?	Same policies, same access controls.	Contractors on personal devices with production access.

8. AI features (if the vendor uses AI on your data)

Question	A good answer	Red flag
8.1 Which AI models or providers process our data?	Named providers, covered as subprocessors.	Unnamed third-party AI.
8.2 Is our data used to train models?	No, or only with explicit opt-in.	Yes by default.
8.3 How do you test AI features for prompt injection and data leakage?	Adversarial testing and output controls.	No testing.

Scoring the answers

- **Approve:** assurance report in scope and current, no red flags on data they will hold.
- **Approve with conditions:** gaps you can cover by contract or by limiting the data they receive. Record the conditions and a review date.
- **Decline or escalate:** red flags on encryption, access or breach notification for a high-risk vendor.

What to do next

1. List your vendors, tier them, and send sections 1 to 4 to every high-risk vendor this month. Ask for their assurance report at the same time.
2. Write your own answers to every question above once, with evidence links, and keep them current.
3. Publish what you can on a trust page, so buyers read before they ask.
4. Where your answer would be a red flag, fix the control rather than the wording.

Want a second pair of eyes? TrazTech runs security and compliance readiness as fixed-scope work for software companies. Book a free 30-minute readiness call at traztech.ca/free-readiness-call, or get The Compliance Brief, one short email every Tuesday, at traztech.ca/brief.