RESILIENTLY

Cybersecurity made clear.

Vendor Risk Questionnaire

A comprehensive questionnaire for assessing third-party vendor cybersecurity and risk management practices.

Free Template from Resiliently

resiliently.co/tools/templates

Version 1.0 | February 2026

Vendor Information

Vendor/Company Name

Primary Contact Name

Contact Email

Contact Phone

Services Provided

Data Types Accessed/Processed

1. Security Governance

Do you have a dedicated security team or officer? If yes, describe the structure.

List current security certifications (SOC 2, ISO 27001, etc.)

When was your last third-party security audit/assessment?

Do you have a documented information security policy? (Attach if possible)

2. Access Control

How do you manage user access to systems and data?

Is multi-factor authentication required for all access? Describe implementation.

How are privileged accounts managed and monitored?

What is your process for revoking access upon employee termination?

3. Data Protection

How is data encrypted at rest? Specify algorithms and key management.

How is data encrypted in transit? Specify protocols used.

Where will our data be stored? List all locations/cloud providers.

What is your data retention and destruction policy?

Do you use subprocessors? If yes, list them and their purpose.

4. Network & Infrastructure Security

Describe your network security controls (firewalls, IDS/IPS, segmentation)

How often are vulnerability scans performed? Who performs them?

What is your patch management process and timeline for critical patches?

Do you have endpoint detection and response (EDR) deployed?

5. Incident Response

Do you have a documented incident response plan?

What is your notification timeline for security incidents affecting customers?

Have you experienced any security incidents in the past 24 months? If yes, describe.

Do you carry cyber insurance? If yes, provide coverage amount.

6. Business Continuity

Describe your backup procedures (frequency, storage, testing)

What is your Recovery Time Objective (RTO)?

What is your Recovery Point Objective (RPO)?

When was your disaster recovery plan last tested?

7. Compliance & Legal

List all compliance frameworks you adhere to (GDPR, HIPAA, PCI-DSS, etc.)

Are you willing to sign a Data Processing Agreement (DPA)?

Do your terms allow for customer security audits or questionnaires?

Are there any pending legal actions related to data breaches?

8. Security Awareness

Do all employees receive security awareness training? How often?

Do you conduct phishing simulations?

Are background checks performed on employees with access to customer data?

Attestation

I certify that the information provided in this questionnaire is accurate and complete to the best of my knowledge.

Name

Title

Signature Date