Vendor Risk Assessment Questionnaire for IT Suppliers

A **vendor risk assessment questionnaire** for IT suppliers evaluates potential security, compliance, and operational risks associated with third-party providers. This tool helps organizations ensure that their IT partners meet necessary standards and mitigate potential vulnerabilities. Effective assessments protect data integrity and maintain business continuity.

General Information

1. Company Name:
2. Address:
3. Primary Contact (Name, Title, Email, Phone):
4. Nature of Products/Services Provided:
5. Years in Business:

Security

1. Do you have an information security policy?

   ☐ Yes ☐ No

2. Are employees trained on IT security best practices?

   ☐ Yes ☐ No

3. Do you perform regular vulnerability assessments and penetration testing?
4. How do you manage user access control and authentication?
5. What encryption methods do you use for data in transit and at rest?

Compliance

1. Are you compliant with relevant standards and regulations (e.g., GDPR, HIPAA, PCI DSS)?
2. Have you undergone any recent audits or assessments? Please provide reports if possible.
3. Do you have documented processes for handling data breaches or incidents?
4. Can you provide a copy of your privacy policy?

Operational Resilience

1. Do you have a disaster recovery and business continuity plan in place?
2. How frequently are these plans tested?
3. Describe your data backup processes and storage locations.
4. Are third-party subcontractors involved in service delivery? If so, how are they vetted?

Risk Management

1. What is your process for identifying and mitigating risks?
2. Do you have a dedicated risk management team?
3. How are risks reported and escalated internally?

References & Documentation

1. Please provide references from other organizations you work with.
2. Attach or link any relevant certifications (e.g., ISO 27001, SOC 2).

Signature

Name: _____

Title: _____

Date: _____