IronRoot
Risk Consultants

Vendor Risk Questionnaire

Third-Party Security Assessment | IronRoot Risk Consultants

Complete this questionnaire for any vendor with access to your systems, data, or facilities. Responses should be provided in writing. Supporting documentation is welcomed where noted.

Vendor Information

Vendor / Company Name:	_____	**Date Completed:**	_____
Primary Contact Name:	_____	**Title:**	_____
Email:	_____	**Phone:**	_____
Services Provided:	_____	**Contract Start Date:**	_____

Section 1: Security Program & Governance

#	Question	Yes	No	N/A	Notes / Evidence
1	Do you have a written information security policy?	[ ]	[ ]	[ ]	
2	Has your security policy been reviewed or updated in the last 12 months?	[ ]	[ ]	[ ]	
3	Do you conduct formal security risk assessments? If yes, how frequently?	[ ]	[ ]	[ ]	
4	Do you have a designated security officer or role responsible for information security?	[ ]	[ ]	[ ]	
5	Do you carry cyber liability insurance? If yes, please provide coverage limits.	[ ]	[ ]	[ ]	
6	Do you have a formal vulnerability management or patch management program?	[ ]	[ ]	[ ]	

Section 2: Access Controls & Authentication

#	Question	Yes	No	N/A	Notes / Evidence
1	Is multi-factor authentication (MFA) enforced for all employees accessing your systems?	[ ]	[ ]	[ ]	
2	Do you enforce MFA on all access to systems that process or store our data?	[ ]	[ ]	[ ]	
3	Do you follow the principle of least privilege when granting access rights?	[ ]	[ ]	[ ]	
4	Do you have a formal user access review process? If yes, how frequently?	[ ]	[ ]	[ ]	
5	Do you have a documented employee offboarding procedure that includes immediate access revocation?	[ ]	[ ]	[ ]	
6	Do you use a privileged access management (PAM) solution for administrative accounts?	[ ]	[ ]	[ ]	

Section 3: Data Protection

#	Question	Yes	No	N/A	Notes / Evidence
1	Do you encrypt data at rest using AES-256 or equivalent?	[ ]	[ ]	[ ]	
2	Do you encrypt data in transit using TLS 1.2 or higher?	[ ]	[ ]	[ ]	
3	Can you describe how you classify and handle sensitive or confidential data?	[ ]	[ ]	[ ]	
4	Do you have a documented data retention and secure disposal policy?	[ ]	[ ]	[ ]	
5	Have you identified all locations where our data may be stored or processed?	[ ]	[ ]	[ ]	
6	Will you notify us within 72 hours of discovering a breach involving our data?	[ ]	[ ]	[ ]	

Section 4: Network Security & Endpoint Protection

#	Question	Yes	No	N/A	Notes / Evidence
1	Do you use endpoint detection and response (EDR) or antivirus on all endpoints?	[ ]	[ ]	[ ]	
2	Do you conduct regular security awareness training for your employees?	[ ]	[ ]	[ ]	

3	Do you segment your network to isolate sensitive systems?	[ ]	[ ]	[ ]	
4	Do you perform regular penetration testing or vulnerability scanning? If yes, how frequently?	[ ]	[ ]	[ ]	
5	Do you have a backup and disaster recovery plan that has been tested?	[ ]	[ ]	[ ]	
6	Do you have a written incident response plan? Has it been exercised in the last 12 months?	[ ]	[ ]	[ ]	

Section 5: Subcontractors & Compliance

#	Question	Yes	No	N/A	Notes / Evidence
1	Do you use any subcontractors or sub-processors who may access our data?	[ ]	[ ]	[ ]	
2	Do your subcontractor agreements include data security and confidentiality requirements?	[ ]	[ ]	[ ]	
3	Have you achieved any security certifications (SOC 2, ISO 27001, PCI DSS)? If yes, please attach.	[ ]	[ ]	[ ]	
4	Are you subject to any regulatory requirements relevant to the services provided to us?	[ ]	[ ]	[ ]	
5	Do you perform security reviews of your own third-party vendors?	[ ]	[ ]	[ ]	

Reviewer Notes

Risk Rating Assigned:	[ ] Critical [ ] High [ ] Medium [ ] Low [ ] Acceptable
Reviewed By:	_____
Review Date:	_____
Next Review Date:	_____
Key Findings:	
Required Remediation:	