Third-Party Due Diligence Review & Security Questionnaire

Vendor Name: _____

Assessment Date: _____

Business Owner: _____

Assessor: _____

Section 1 – Governance & Compliance

1. Do you maintain formal information security policies approved by management? (Yes/No)
2. Do you undergo independent audits (SOC 2, ISO 27001, etc.)? Please provide latest report.
3. Is there a designated security officer or team responsible for cybersecurity governance?
4. Do you perform annual risk assessments?
5. Do you maintain a vendor risk management program for your subprocessors?

Evidence Reviewed:

- SOC 2 Report: _____

- ISO 27001 Certificate: _____

- Risk Assessment Summary: _____

- Security Policy Documentation: _____

Section 2 – Identity & Access Management

6. Is Multi-Factor Authentication (MFA) enforced for all administrative accounts?
7. Is role-based access control (RBAC) implemented?
8. Are privileged accounts uniquely assigned (no shared accounts)?
9. Are access reviews conducted at least quarterly?
10. Are terminated users deprovisioned within 24 hours?

Evidence Reviewed:

- Access Control Policy: _____

- MFA Configuration Screenshot: _____

- Access Review Documentation: _____

Section 3 – Data Protection & Encryption

11. Is data encrypted at rest using industry-standard encryption (AES-256 or equivalent)?
12. Is data encrypted in transit using TLS 1.2+?
13. Is sensitive data tokenized, masked, or minimized where possible?
14. Are secure key management practices implemented?
15. Is data retention formally defined and enforced?

Evidence Reviewed:

- Encryption Architecture Diagram: _____

- Key Management Procedure: _____

- Data Retention Policy: _____

Section 4 – Logging, Monitoring & Incident Response

16. Are security logs retained for at least 90 days?
17. Is centralized logging or SIEM implemented?
18. Are security alerts actively monitored?
19. Is there a documented incident response plan?
20. Is breach notification provided within a defined SLA (e.g., 72 hours)?

Evidence Reviewed:

- Logging Retention Policy: _____

- Incident Response Plan: _____

- IR Test Results: _____

Section 5 – Business Continuity & Disaster Recovery

21. Is there a documented Business Continuity Plan (BCP)?
22. Is there a Disaster Recovery Plan (DRP)?
23. Are DR tests conducted annually?
24. What are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?

Evidence Reviewed:

- BCP Document: _____

- DR Test Report: _____

Section 6 – Subprocessors & Regulatory Considerations

25. Do you maintain a current list of subprocessors?

26. Are subprocessors contractually obligated to meet security requirements?
27. Are data processing agreements (DPAs) in place?
28. Do you sign Business Associate Agreements (BAA) if handling PHI?
29. Do you support PCI DSS compliance if processing payment data?

Evidence Reviewed:

- Subprocessor List: _____

- DPA Template: _____

- BAA (if applicable): _____

Assessor Notes & Findings

Summary of identified gaps, control weaknesses, or observations:

Overall Due Diligence Outcome

☐ Low Risk

☐ Medium Risk

☐ High Risk

☐ Critical Risk

Assessor Signature: _____

Date: _____

Created by: Jodelis Diaz