Third-Party Due Diligence Questionnaire (SOC 2 Mapped)

Vendor Name: ________________________

Assessment Date: ______________________

Business Owner: _______________________

Assessor: _____________________________

This questionnaire is mapped to the SOC 2 Trust Services Criteria (TSC) to evaluate vendor controls relevant to Security, Availability, and Confidentiality.

Section CC – Common Criteria (Security)

1. CC1.1 – Does management demonstrate commitment to integrity and ethical values?
2. CC2.1 – Is a formal risk assessment performed at least annually?
3. CC3.2 – Are security policies formally documented and approved?
4. CC4.1 – Are monitoring activities performed to detect control failures?
5. CC5.2 – Are control deficiencies evaluated and remediated timely?
6. CC6.1 – Is logical access restricted based on job responsibilities (RBAC)?
7. CC6.2 – Is Multi-Factor Authentication enforced for privileged users?
8. CC6.3 – Are user access reviews conducted periodically?
9. CC7.1 – Are system vulnerabilities identified and remediated?
10. CC7.2 – Is logging and monitoring implemented to detect security events?
11. CC7.3 – Is there a documented incident response plan?

Evidence Reviewed:

- SOC 2 Type II Report: _______________________

- Security Policy Documentation: ________________

- Vulnerability Scan Reports: __________________

- Incident Response Plan & Test Results: ________

Section A – Availability

12. A1.1 – Are availability commitments defined in SLAs?
13. A1.2 – Is system performance monitored against availability targets?
14. A1.3 – Is there a documented Disaster Recovery Plan (DRP)?
15. A1.4 – Are DR tests conducted at least annually?
16. A1.5 – Are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined?

Evidence Reviewed:

- SLA Documentation: ________________________

- DR Test Report: ___________________________

- Monitoring Dashboard Screenshot: ____________

Section C – Confidentiality

17. C1.1 – Is confidential data identified and classified?
18. C1.2 – Is confidential data encrypted at rest (e.g., AES-256)?
19. C1.3 – Is confidential data encrypted in transit (TLS 1.2+)?
20. C1.4 – Are data retention and disposal policies defined?
21. C1.5 – Are subprocessors contractually required to protect confidential data?

Evidence Reviewed:

- Data Classification Policy: _________________

- Encryption Architecture Documentation: _______

- Subprocessor List & Agreements: _____________

Section P – Privacy (If Applicable)

22. P1.1 – Are privacy notices provided to data subjects?
23. P2.1 – Is personal data collected, used, and retained per policy?
24. P3.1 – Are data subject access requests (DSARs) supported?
25. P4.1 – Are privacy incidents tracked and reported?

Evidence Reviewed (If Applicable):

- Privacy Policy: ____________________________

- DSAR Procedure: ___________________________

- Privacy Incident Log: ______________________

Assessor Notes & SOC 2 Alignment Summary

Document control gaps, observations, and alignment with SOC 2 criteria below:

Overall SOC 2 Due Diligence Outcome

☐ Controls appear suitably designed

☐ Minor gaps identified (remediation required)

☐ Significant deficiencies identified

☐ Controls not suitably designed

Assessor Signature: ______________________

Date: ______________________

Created by: Jodelis Diaz