Third-Party Due Diligence Questionnaire (SOC 2 Mapped)

Vendor Name: PayrollCo

Assessment Date: January 2026

Business Owner: HR Director

Assessor: GRC Analyst

Assessment Scope: PayrollCo provides payroll processing services handling regulated employee PII including SSN and banking data. Assessment focuses on SOC 2 Security, Availability, and Confidentiality criteria.

Section CC – Common Criteria (Security)

- CC1.1 – YES. Management maintains documented security policies and a code of conduct.
- CC2.1 – YES. Annual enterprise risk assessment performed (SOC 2 reviewed).
- CC3.2 – YES. Information security policies formally documented and approved.
- CC4.1 – PARTIAL. Monitoring activities exist but log retention limited to 7 days.
- CC5.2 – YES. Control deficiencies tracked through internal ticketing system.
- CC6.1 – YES. RBAC enforced for application access.
- CC6.2 – YES. MFA enforced for administrative access.
- CC6.3 – YES. Quarterly user access reviews performed.
- CC7.1 – PARTIAL. Vulnerability scans performed; patch SLA documentation incomplete.
- CC7.2 – PARTIAL. Logging implemented but not centrally retained ≥90 days.
- CC7.3 – YES. Incident Response Plan documented; 72-hour notification commitment.

Evidence Reviewed:

- SOC 2 Type II Report (Security & Availability criteria)

- Access Control Policy

- Vulnerability Scan Summary

- Incident Response Plan

Section A – Availability

- A1.1 – YES. SLA defines 99.9% uptime commitment.
- A1.2 – YES. System uptime monitored via cloud monitoring platform.
- A1.3 – YES. Disaster Recovery Plan documented.
- A1.4 – YES. Annual DR test performed (summary reviewed).

- A1.5 – YES. RTO = 8 hours; RPO = 4 hours.

Evidence Reviewed:

- SLA Documentation

- DR Test Report Summary

- Monitoring Dashboard Evidence

Section C – Confidentiality

- C1.1 – YES. Data classification policy identifies regulated payroll data as Confidential/Restricted.
- C1.2 – YES. AES-256 encryption at rest implemented in cloud storage.
- C1.3 – YES. TLS 1.2+ encryption enforced for data in transit.
- C1.4 – PARTIAL. Data retention policy exists but lacks detailed deletion verification controls.
- C1.5 – PARTIAL. Subprocessor list provided but no formal change notification process.

Evidence Reviewed:

- Encryption Architecture Documentation

- Data Retention Policy

- Subprocessor Listing

Key Findings Identified

- High: Audit logs retained only 7 days; no SIEM export capability.
- Medium: No formal subprocessor change notification process.
- Medium: Patch SLA documentation incomplete.

Overall SOC 2 Due Diligence Outcome

Controls appear suitably designed in most areas; however, logging retention and subprocessor transparency gaps result in HIGH residual risk until remediation is completed.

Final Determination: Approve with Conditions

Monitoring Requirement: Quarterly review until remediation closure.

Assessor Signature: _____

Date: _____

Created by: Jodelis Diaz