Vendor Security Questionnaire – Responses

Section 1: General Information

1. Organization Name: CloudSecure Solutions Inc.

2. Security Contact: John Doe, Chief Security Officer (john.doe@cloudsecure.com, 555-123-4567)

3. Certifications: SOC 2, GDPR compliance, and ISO 27001-certified.

Section 2: Data Security

4. Yes, we use AES-256 encryption for both data storage and transmission.

5. Access is role-based, and we require multi-factor authentication (MFA) for all employees accessing sensitive data.

6. Yes, we use a Security Information and Event Management (SIEM) system for real-time monitoring of unauthorized access attempts.

Section 3: Incident Response

7. Yes, we have a documented incident response plan that is reviewed annually.

8. We typically respond to incidents within 2 hours of detection.

9. No security breaches have occurred in the past 12 months.

Section 4: Employee Training

10. Yes, all employees undergo mandatory security training every quarter.

11. Phishing simulations are conducted twice a year.

Section 5: Regulatory Compliance

12. We comply with GDPR, HIPAA (for healthcare clients), and CCPA.

13. Data requests are managed by our compliance team, which ensures proper documentation and secure handling of the requested information.

Section 6: Vendor Security

14. Yes, we use third-party data centers that meet SOC 2 and ISO 27001 standards.

15. Subcontractors are required to sign a security agreement and follow our vendor management policy.