SecureCloud Technologies Inc.

Vendor Security Assessment Response Document

Document Version 2.0 - January 2025

SECTION 1: INFORMATION SECURITY & CYBERSECURITY

Question: What is your employee security awareness training program?

We provide annual security awareness training to all employees. The training program includes phishing simulation exercises, password security best practices, and data handling procedures. All employees must complete the training within 30 days of hire and annually thereafter. Training completion is tracked through our learning management system.

Question: Do you maintain a dedicated cybersecurity team or Chief Information Security Officer?

No, we do not maintain a dedicated cybersecurity team or Chief Information Security Officer. Our IT department handles security-related tasks as part of their general responsibilities.

SECTION 2: DATA PRIVACY & PROTECTION

Question: Are you compliant with GDPR, CCPA, and other applicable data privacy regulations?

Yes, we are compliant with GDPR and CCPA regulations. We have implemented privacy policies and procedures to ensure compliance with applicable data protection regulations.

Question: Do you have a designated Data Protection Officer (DPO)?

No, we do not have a designated Data Protection Officer. Privacy matters are handled by our legal department.

SECTION 3: FINANCIAL STABILITY & BUSINESS CONTINUITY

Question: Have you experienced any bankruptcy, insolvency, or financial restructuring in the past 5 years?

No, we have not experienced any bankruptcy, insolvency, or financial restructuring in the past 5 years.

Question: Do you maintain appropriate business insurance including cyber liability coverage?

Yes, we maintain business insurance including general liability and professional liability coverage. Our cyber liability coverage is $2 million per occurrence.

Question: Do you conduct regular business continuity testing and drills?

No, we do not conduct regular business continuity testing and drills. We have basic backup procedures but no formal testing schedule.

SECTION 4: OPERATIONAL RISK & SERVICE DELIVERY

Question: Do you provide 24/7 technical support and monitoring?

No, we provide technical support during business hours only (Monday through Friday, 9 AM to 5 PM EST). After-hours support is available on an emergency basis.

Question: Do you maintain detailed operational documentation and runbooks?

Yes, we maintain operational documentation including standard operating procedures, user manuals, and system configuration guides. Documentation is reviewed and updated quarterly.

Question: Do you have established escalation procedures for critical incidents?

Yes, we have established escalation procedures for critical incidents. Level 1 issues are handled by our support team, with escalation to senior technicians and management as needed.

SECTION 5: COMPLIANCE & REGULATORY ADHERENCE

Question: Are you compliant with industry-specific regulations relevant to our business?

Yes, we are compliant with industry-specific regulations relevant to our business operations. We monitor regulatory requirements and update our practices accordingly.

Question: Do you maintain a dedicated compliance officer or legal team?

No, we do not maintain a dedicated compliance officer. Compliance activities are managed by our operations team with external legal counsel as needed.

SECTION 6: LEGAL & CONTRACTUAL CONSIDERATIONS

Question: Are you currently involved in any material litigation or legal disputes?

No, we are not currently involved in any material litigation or legal disputes.

Question: Do you maintain appropriate professional liability and errors & omissions insurance?

Yes, we maintain professional liability and errors & omissions insurance with $1 million coverage per claim.

SECTION 7: THIRD-PARTY MANAGEMENT

Question: Do you have a formal third-party risk management program?

No, we do not have a formal third-party risk management program. We evaluate vendors on a case-by-case basis during procurement.

Question: Do you maintain an updated inventory of all third-party relationships?

Yes, we maintain an inventory of all third-party relationships including vendors, suppliers, and service providers. The inventory is updated annually.

SECTION 8: ENVIRONMENTAL & SOCIAL GOVERNANCE

Question: Do you have established environmental sustainability policies and practices?

Yes, we have established environmental sustainability policies including energy-efficient office practices and electronic document management to reduce paper usage.

Question: Do you maintain ethical business practices and anti-corruption policies?

Yes, we maintain ethical business practices and anti-corruption policies. All employees sign a code of conduct agreement upon hiring.

SECTION 9: TECHNOLOGY INFRASTRUCTURE

Question: Do you use cloud infrastructure with major providers (AWS, Azure, GCP)?

Yes, we use cloud infrastructure with Amazon Web Services (AWS) as our primary cloud provider for hosting applications and data storage.

Question: Do you maintain separate development, testing, and production environments?

Yes, we maintain separate development, testing, and production environments with appropriate access controls between environments.

Question: Do you implement automated monitoring and alerting for system performance?

Yes, we implement automated monitoring and alerting for system performance using CloudWatch and custom monitoring scripts.

SECTION 10: HUMAN RESOURCES & PERSONNEL SECURITY

Question: Do you conduct background checks on all employees with access to sensitive data?

No, we do not conduct background checks on all employees. Background checks are performed only for employees in senior management positions.

Question: Do you have established policies for remote work and bring-your-own-device (BYOD)?

Yes, we have established policies for remote work and bring-your-own-device (BYOD). Employees must use company-approved security software on personal devices.

Question: Do you provide regular security training and awareness programs for staff?

Yes, we provide regular security training and awareness programs for staff. Training is conducted annually with additional updates as needed.

SECTION 11: ADDITIONAL INFORMATION

Company Founded: 2019 **Number of Employees:** 85 **Primary Services:** Cloud hosting, data analytics, web applications **Geographic Presence:** North America **Annual Revenue:** $12 million (2024)

DOCUMENT CONTROL

Document Classification: Confidential **Prepared By:** Operations Team **Reviewed By:** Legal Department
Approved By: Chief Executive Officer **Next Review Date:** July 2025

END OF DOCUMENT