Third-Party Vendor Risk Assessment Procedure

Nexus Intelligent Systems, Inc.

Compliance & Enterprise Risk Management Policy

1. PURPOSE

1 This Third-Party Vendor Risk Assessment Procedure ("Procedure") establishes a comprehensive framework for evaluating, monitoring, and managing risks associated with external vendors, suppliers, and service providers engaged by Nexus Intelligent Systems, Inc. (the "Company").

2 The primary objectives of this Procedure are to:

a) Mitigate potential operational, financial, legal, and cybersecurity risks

b) Ensure vendor alignment with Company standards and regulatory requirements

c) Establish a systematic approach to vendor due diligence and ongoing assessment

2. SCOPE

1 This Procedure applies to all third-party vendors, contractors, consultants, and service providers who:

a) Have access to Company systems or confidential information

b) Provide critical services or technologies

c) Represent potential strategic or operational risk exposure

2 The Procedure encompasses the entire vendor lifecycle, including:

- Initial vendor selection
- Pre-engagement risk assessment
- Ongoing performance and risk monitoring
- Periodic vendor re-evaluation

3. RISK ASSESSMENT METHODOLOGY

1 Vendor Risk Classification

a) Critical Risk Vendors: Vendors with direct access to sensitive systems or data

b) High Risk Vendors: Vendors providing essential services with potential significant impact

c) Moderate Risk Vendors: Vendors with limited system access or peripheral services

d) Low Risk Vendors: Vendors with minimal interaction or standardized services

2 Risk Assessment Criteria

The Company shall evaluate vendors across the following dimensions:

- Cybersecurity capabilities
- Financial stability
- Regulatory compliance
- Data protection practices
- Business continuity capabilities
- Operational performance metrics

4. DUE DILIGENCE PROCESS

1 Pre-Engagement Assessment

a) Comprehensive vendor questionnaire

b) Background and financial documentation review

c) Security and compliance documentation validation

d) Reference and reputation assessment

2 Initial Risk Scoring

Vendors will be evaluated using a standardized risk scoring matrix with weighted criteria:

- Information Security: 30%
- Financial Stability: 25%
- Regulatory Compliance: 20%
- Operational Performance: 15%
- Business Continuity: 10%

5. ONGOING MONITORING

1 Periodic Review Requirements

a) Critical Risk Vendors: Quarterly comprehensive assessments

b) High Risk Vendors: Semi-annual detailed reviews

c) Moderate Risk Vendors: Annual comprehensive evaluations

d) Low Risk Vendors: Biennial light-touch assessments

2 Continuous Risk Tracking

The Company will maintain a dynamic vendor risk register with real-time updates and escalation protocols.

6. REMEDIATION AND TERMINATION

1 Risk Mitigation Protocols

a) Vendors failing to meet minimum risk thresholds will receive formal remediation notices

b) Corrective action plans with specific timelines and performance metrics

c) Right to suspend or terminate vendor relationships for persistent non-compliance

7. DOCUMENTATION AND RECORD KEEPING

1 All vendor risk assessments, communications, and evaluations shall be:

a) Documented in a centralized vendor management system

b) Maintained for a minimum of seven (7) years

c) Subject to periodic internal and external audit review

8. LEGAL DISCLAIMER

1 This Procedure represents a framework and does not constitute a contractual obligation. The Company reserves the right to modify, suspend, or terminate this Procedure at its sole discretion.

9. APPROVAL AND IMPLEMENTATION

1 Effective Date: January 22, 2024

2 Approved By: Michael Chen, Chief Technology Officer

3 Authorized Signature: [Digital Signature]

10. CONTACT INFORMATION

Risk Management Department

Nexus Intelligent Systems, Inc.

Email: vendor.risk@nexusai.com

Phone: (415) 555-0187