Third-Party Vendor Risk Management Protocol

Nexus Intelligent Systems, Inc.

1. PURPOSE AND SCOPE

1 This Third-Party Vendor Risk Management Protocol ("Protocol") establishes comprehensive guidelines for identifying, assessing, monitoring, and mitigating risks associated with external vendor relationships at Nexus Intelligent Systems, Inc. (the "Company").

2 The Protocol applies to all third-party vendors, contractors, service providers, and strategic partners who:

a) Have access to Company systems or data

b) Provide critical services or technologies

c) Interact with sensitive corporate infrastructure

d) Represent potential cybersecurity or operational risk vectors

2. VENDOR CLASSIFICATION FRAMEWORK

1 Vendor Risk Tiers

- Tier 1: Critical Vendors (High Risk/Strategic Importance)
- Tier 2: Operational Vendors (Moderate Risk)
- Tier 3: Peripheral Vendors (Low Risk)

2 Risk Classification Criteria

a) Data Access Level

b) Financial Impact

c) Cybersecurity Exposure

d) Regulatory Compliance Requirements

e) Strategic Alignment

3. PRE-ENGAGEMENT RISK ASSESSMENT

1 Initial Vendor Screening

- Comprehensive background investigation
- Financial stability verification

- Cybersecurity capability assessment
- Compliance documentation review

2 Required Documentation

- SOC 2 Type II Certification
- Cybersecurity Insurance Evidence
- Business Continuity Plan
- Data Protection and Privacy Policies
- Regulatory Compliance Certifications

4. ONGOING VENDOR MONITORING PROTOCOL

1 Periodic Risk Reassessment

- Tier 1 Vendors: Quarterly comprehensive review
- Tier 2 Vendors: Semi-annual detailed assessment
- Tier 3 Vendors: Annual lightweight review

2 Performance and Risk Metrics

- Security Incident Response Time
- Service Level Agreement (SLA) Compliance
- Data Protection Effectiveness
- Financial Stability Indicators

5. CONTRACTUAL RISK MITIGATION

1 Mandatory Contract Provisions

a) Comprehensive Indemnification Clauses

b) Explicit Data Protection Requirements

c) Right to Audit Provisions

d) Immediate Termination Conditions

e) Cybersecurity Performance Guarantees

2 Vendor Performance Bonds

- Tiered financial guarantees based on risk classification
- Mandatory cyber liability insurance requirements

- Performance penalty mechanisms

6. INCIDENT RESPONSE AND REMEDIATION

1 Vendor Security Incident Protocol

- Immediate notification requirements
- Mandatory 24-hour incident reporting
- Collaborative remediation process
- Potential contract suspension mechanisms

2 Risk Mitigation Escalation

- Defined communication channels
- Executive oversight triggers
- Potential vendor relationship termination process

7. COMPLIANCE AND GOVERNANCE

1 Internal Oversight

- Chief Information Security Officer (CISO) ultimate accountability
- Cross-functional vendor risk committee
- Annual protocol review and update

2 Regulatory Alignment

- NIST SP 800-161 Cybersecurity Supply Chain Risk Management
- GDPR Vendor Management Requirements
- CCPA Third-Party Data Protection Standards

8. DISCLAIMER AND LIMITATIONS

1 This Protocol represents a comprehensive risk management framework but does not guarantee absolute protection against all potential vendor-related risks.

2 The Company reserves the right to modify this Protocol at its sole discretion.

EXECUTION

Approved and Executed:

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.

Date: January 22, 2024