Cybersecurity and Risk Management Addendum

PREAMBLE

This Cybersecurity and Risk Management Addendum (the "Addendum") is executed on January 22, 2024, by and between Nexus Intelligent Systems, Inc., a Delaware corporation with principal offices at 1200 Innovation Park Drive, San Jose, California 95134 (hereinafter referred to as "Nexus" or the "Company").

1. DEFINITIONS

1 "Confidential Information" shall mean all proprietary technical, business, and operational data owned or controlled by Nexus, including but not limited to:

a) Source code and algorithmic designs

b) Client engagement records

c) Machine learning model architectures

d) Network infrastructure configurations

e) Predictive analytics methodologies

2 "Cybersecurity Event" means any confirmed unauthorized access, data breach, system compromise, or potential security vulnerability that could materially impact the Company's technological infrastructure or intellectual property.

2. CYBERSECURITY GOVERNANCE

1 Information Security Framework

The Company shall maintain a comprehensive information security program that includes:

a) Annual third-party cybersecurity assessments

b) Quarterly vulnerability scanning and penetration testing

c) Multi-factor authentication for all critical systems

d) Endpoint detection and response (EDR) mechanisms

e) Continuous security monitoring and incident response protocols

2 Data Protection Standards

Nexus commits to implementing and maintaining:

a) ISO 27001 information security management standards

b) NIST Cybersecurity Framework compliance

c) Advanced encryption protocols for data at rest and in transit

d) Secure development lifecycle for all proprietary software platforms

3. RISK MANAGEMENT PROTOCOLS

1 Threat Detection and Response

The Company shall:

a) Maintain a dedicated cybersecurity operations center (SOC)

b) Implement real-time threat intelligence monitoring

c) Develop and regularly update comprehensive incident response plans

d) Conduct bi-annual tabletop security simulation exercises

2 Third-Party Risk Management

Nexus will:

a) Conduct rigorous vendor security assessments

b) Require contractual cybersecurity compliance from all critical vendors

c) Implement continuous vendor risk monitoring

d) Maintain a centralized vendor risk management database

4. COMPLIANCE AND REPORTING

1 Regulatory Compliance

The Company shall maintain compliance with:

a) GDPR data protection regulations

b) CCPA privacy requirements

c) HIPAA security standards (where applicable)

d) Industry-specific cybersecurity regulations

2 Reporting Requirements

Nexus commits to:

a) Immediate reporting of any significant cybersecurity events

b) Quarterly comprehensive security status reports

c) Annual independent cybersecurity audit

d) Transparent disclosure of material security incidents

5. TECHNOLOGICAL SAFEGUARDS

1 Infrastructure Protection

The Company shall maintain:

a) Redundant cloud and on-premise infrastructure

b) Geographically distributed backup systems

c) Advanced intrusion prevention systems

d) Regular system patch and update management

2 Access Control

Nexus will implement:

a) Role-based access control (RBAC)

b) Principle of least privilege

c) Comprehensive user authentication mechanisms

d) Regular access rights review and reconciliation

6. LIMITATION OF LIABILITY

1 Notwithstanding any provisions herein, the Company's total aggregate liability for any cybersecurity-related claims shall not exceed the lesser of:

a) Actual direct damages

b) $500,000 per incident

c) Total annual contract value

7. MISCELLANEOUS

1 This Addendum shall be governed by and construed in accordance with the laws of the State of California.

2 This document represents the entire understanding between parties regarding cybersecurity risk management.

EXECUTION

Executed this 22nd day of January, 2024.

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.