Cybersecurity Risk Management Framework

Nexus Intelligent Systems, Inc.

1. PURPOSE AND SCOPE

1 This Cybersecurity Risk Management Framework ("Framework") establishes comprehensive protocols for managing, mitigating, and responding to cybersecurity risks within Nexus Intelligent Systems, Inc. (the "Company").

2 The Framework applies to all corporate assets, digital infrastructure, employee interactions, third-party vendor relationships, and technological ecosystems supporting the Company's AI-driven predictive maintenance and digital transformation platforms.

2. GOVERNANCE AND ORGANIZATIONAL STRUCTURE

1 Cybersecurity Governance

- The Chief Technology Officer (CTO) shall serve as the primary executive responsible for cybersecurity strategy and implementation.
- A dedicated Cybersecurity Steering Committee shall be established, comprising:

a) CTO (Committee Chair)

b) Chief Information Security Officer

c) Chief Compliance Officer

d) Senior Legal Counsel

e) Head of IT Infrastructure

2 Roles and Responsibilities

- Executive Leadership: Strategic oversight and resource allocation
- Cybersecurity Team: Operational implementation and continuous monitoring
- Department Heads: Compliance and risk awareness within respective divisions
- All Employees: Adherence to security protocols and immediate incident reporting

3. RISK ASSESSMENT METHODOLOGY

1 Comprehensive Risk Identification

- Annual comprehensive cybersecurity risk assessment

- Quarterly threat landscape analysis
- Continuous vulnerability scanning and penetration testing
- Third-party vendor security evaluation

2 Risk Classification Matrix

- Critical Risk: Immediate mitigation required
- High Risk: Remediation within 30 days
- Moderate Risk: Remediation within 90 days
- Low Risk: Monitoring and periodic review

4. TECHNICAL CONTROL FRAMEWORK

1 Infrastructure Security

- Multi-layered network segmentation
- Advanced endpoint protection
- Zero-trust architecture implementation
- Encrypted communication protocols
- Regular system patch management

2 Access Control Mechanisms

- Multi-factor authentication
- Role-based access controls
- Privileged access management
- Comprehensive user activity logging
- Automated access review processes

5. INCIDENT RESPONSE PROTOCOL

1 Incident Classification

- Categorization based on potential business impact
- Predefined response workflows
- Clear escalation procedures

2 Response Team Composition

- Incident Response Team

- External Forensic Specialists
- Legal and Compliance Representatives
- Executive Leadership Liaison

3 Incident Management Workflow

- Detection
- Containment
- Eradication
- Recovery
- Post-Incident Analysis

6. COMPLIANCE AND REGULATORY ALIGNMENT

1 Regulatory Frameworks

- NIST Cybersecurity Framework
- ISO 27001 Information Security Standards
- GDPR Data Protection Guidelines
- CCPA Privacy Compliance

2 Audit and Verification

- Annual third-party security audits
- Continuous compliance monitoring
- Documented remediation tracking

7. TRAINING AND AWARENESS

1 Mandatory Security Training

- Annual comprehensive cybersecurity training
- Role-specific security awareness programs
- Simulated phishing and social engineering exercises

2 Knowledge Management

- Centralized security knowledge repository
- Regular communication of emerging threats
- Incentive programs for security consciousness

8. VENDOR AND THIRD-PARTY RISK MANAGEMENT

1 Vendor Security Assessment

- Comprehensive security questionnaires
- Mandatory security documentation
- Ongoing vendor risk monitoring

2 Contract Security Requirements

- Minimum security standards
- Right to audit clauses
- Incident reporting obligations

9. DISCLAIMER AND LIMITATIONS

1 This Framework represents a best-effort approach to cybersecurity risk management and does not guarantee absolute protection against all potential threats.

2 The Company reserves the right to modify this Framework as technological landscapes and threat environments evolve.

10. EXECUTION

Approved and Executed:

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.

Date: January 22, 2024