Data Breach Response and Mitigation Plan

Nexus Intelligent Systems, Inc.

1. PURPOSE AND SCOPE

1 This Data Breach Response and Mitigation Plan ("Plan") establishes the comprehensive protocol for addressing potential cybersecurity incidents for Nexus Intelligent Systems, Inc. (the "Company"), specifically designed to manage, contain, and remediate data security breaches affecting the Company's digital infrastructure, client data, and proprietary systems.

2 The Plan applies to all Company employees, contractors, vendors, and third-party service providers with access to Company digital assets and confidential information.

2. DEFINITIONS

1 "Data Breach" shall mean any unauthorized access, disclosure, acquisition, or potential compromise of sensitive, protected, or confidential digital information maintained by the Company.

2 "Sensitive Information" includes, but is not limited to:

a) Personal identifiable information (PII)

b) Corporate financial data

c) Client proprietary information

d) Intellectual property

e) System configuration details

f) Authentication credentials

3. INCIDENT RESPONSE TEAM

1 The Company shall maintain a dedicated Incident Response Team ("IRT") with the following composition:

- Chief Information Security Officer (Primary Coordinator)
- Chief Technology Officer
- Legal Counsel
- Human Resources Representative
- External Cybersecurity Consultant

2 The IRT shall convene immediately upon detection of a potential data breach, with predefined communication protocols and escalation procedures.

4. BREACH DETECTION AND INITIAL ASSESSMENT

1 Detection Mechanisms:

a) Continuous network monitoring systems

b) Automated intrusion detection software

c) Security information and event management (SIEM) platforms

d) Employee reporting channels

2 Initial Assessment Protocol:

- Immediate system isolation
- Forensic evidence preservation
- Preliminary impact evaluation
- Threat vector identification

5. CONTAINMENT STRATEGIES

1 Immediate Containment Actions:

a) Disconnect compromised systems

b) Revoke and reset authentication credentials

c) Block identified malicious IP addresses

d) Implement emergency access restrictions

2 Technical Containment Measures:

- Network segmentation
- Enhanced firewall configurations
- Temporary system quarantine
- Comprehensive log analysis

6. NOTIFICATION AND COMMUNICATION PROTOCOLS

1 Internal Notification:

- Immediate communication to executive leadership
- Structured briefing for Board of Directors

- Confidential employee communication

2 External Notification:

- Client communication strategy
- Regulatory compliance reporting
- Potential law enforcement engagement

7. REMEDIATION AND RECOVERY

1 Systematic Remediation Steps:

a) Complete system vulnerability assessment

b) Patch and update security infrastructure

c) Comprehensive system restoration

d) Enhanced monitoring implementation

2 Long-Term Mitigation:

- Security infrastructure upgrades
- Enhanced employee training programs
- Periodic third-party security audits

8. LEGAL AND COMPLIANCE CONSIDERATIONS

1 The Company shall maintain full documentation of breach response activities to support potential legal or regulatory inquiries.

2 All actions shall comply with applicable data protection regulations, including but not limited to GDPR, CCPA, and industry-specific compliance requirements.

9. CONFIDENTIALITY AND LIMITATIONS

1 This Plan represents confidential intellectual property of Nexus Intelligent Systems, Inc. and is not to be distributed externally without explicit written consent.

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

10. EXECUTION

Approved and Executed:

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.

Date: January 22, 2024