Data Handling and Privacy Protection Procedure

Nexus Intelligent Systems, Inc.

Effective Date: January 22, 2024

1. PURPOSE AND SCOPE

1 This Data Handling and Privacy Protection Procedure ("Procedure") establishes comprehensive guidelines for the management, protection, and secure processing of confidential and sensitive information within Nexus Intelligent Systems, Inc. (the "Company").

2 The purpose of this Procedure is to:

a) Ensure compliance with applicable data protection regulations

b) Establish clear protocols for data management

c) Mitigate risks associated with data breaches and unauthorized disclosures

d) Protect the intellectual property and confidential information of the Company and its clients

2. DEFINITIONS

1 "Confidential Information" shall mean any proprietary or sensitive data, including but not limited to:

a) Client datasets

b) Predictive analytics algorithms

c) Machine learning model configurations

d) Internal strategic documents

e) Financial and operational metrics

2 "Sensitive Personal Information" refers to individually identifiable information that, if disclosed, could potentially cause harm to an individual, including:

a) Government-issued identification numbers

b) Financial account details

c) Health-related information

d) Biometric data

3. DATA CLASSIFICATION FRAMEWORK

1 The Company shall implement a multi-tiered data classification system:

a) Public Information

b) Internal Use Information

c) Confidential Information

d) Restricted Information

2 Each data classification level shall have specific handling, storage, and access protocols.

4. ACCESS CONTROL MECHANISMS

1 Data Access Principles:

a) Principle of Least Privilege

b) Role-Based Access Control (RBAC)

c) Multi-Factor Authentication (MFA)

2 Access Management Requirements:

- Mandatory quarterly access reviews
- Immediate access revocation upon employee separation
- Comprehensive audit logging of data access events

5. DATA PROTECTION TECHNICAL CONTROLS

1 Encryption Standards:

a) AES-256 encryption for data at rest

b) TLS 1.3 for data in transit

c) Mandatory encryption for all portable devices

2 Network Security Protocols:

- Continuous network monitoring
- Intrusion detection systems
- Regular vulnerability assessments
- Segmented network architecture

6. INCIDENT RESPONSE PROTOCOL

1 Data Breach Response Timeline:

- Immediate detection and containment
- Comprehensive forensic investigation within 24 hours
- Mandatory client and regulatory notifications within 72 hours

2 Incident Documentation Requirements:

a) Detailed incident report

b) Root cause analysis

c) Remediation strategy

d) Preventative recommendations

7. THIRD-PARTY VENDOR MANAGEMENT

1 Vendor Assessment Criteria:

- Comprehensive security questionnaires
- Mandatory SOC 2 Type II compliance
- Annual security audits
- Contractual data protection obligations

8. TRAINING AND AWARENESS

1 Mandatory annual data protection training for all employees

2 Quarterly cybersecurity awareness updates

3 Simulated phishing and social engineering tests

9. COMPLIANCE AND ENFORCEMENT

1 Violations of this Procedure may result in:

a) Disciplinary action

b) Potential termination of employment

c) Legal prosecution for severe breaches

10. DOCUMENT ADMINISTRATION

1 This Procedure shall be reviewed annually

2 Modifications require approval from the Chief Compliance Officer and Chief Technology Officer

11. SIGNATURES

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.

Michael Chen

Chief Technology Officer

Nexus Intelligent Systems, Inc.

Date of Execution