

Corporate Record Retention and Management Policy

Nexus Intelligent Systems, Inc.

1. PURPOSE AND SCOPE

1 This Corporate Record Retention and Management Policy ("Policy") establishes comprehensive guidelines for the systematic management, preservation, and disposition of corporate records for Nexus Intelligent Systems, Inc. (the "Company").

2 The Policy applies to all corporate records, regardless of medium, created or received by employees, contractors, executives, and board members in the course of conducting Company business.

2. DEFINITIONS

1 "Corporate Records" shall mean all documents, electronic files, communications, and information assets that document the Company's business operations, legal obligations, financial transactions, and strategic activities.

2 "Retention Period" refers to the prescribed duration for maintaining specific categories of corporate records as mandated by legal, regulatory, or operational requirements.

3 "Confidential Records" are documents containing sensitive proprietary information, intellectual property, financial data, or personally identifiable information requiring heightened protection.

3. RECORD CLASSIFICATION AND RETENTION PERIODS

1 Financial Records

- Financial statements: Permanent retention
- Tax returns and supporting documentation: 7 years
- Audit reports: 10 years
- Expense reports: 7 years

2 Legal and Compliance Documents

- Corporate formation documents: Permanent
- Board meeting minutes: Permanent
- Contracts: 10 years post-expiration

- Intellectual property registrations: Permanent
- Litigation files: 10 years post-resolution

3 Human Resources Records

- Employee personnel files: 7 years post-employment
- Payroll records: 7 years
- Benefits documentation: 6 years
- Recruitment and hiring records: 3 years

4 Technology and Operational Records

- Software development documentation: 7 years
- Client project files: 7 years
- System configuration records: 5 years
- Cybersecurity incident reports: 7 years

4. DIGITAL RECORD MANAGEMENT

1 Electronic Storage Requirements

- All digital records must be stored on secure, encrypted enterprise-grade storage systems
- Implement redundant backup protocols with minimum 99.99% availability
- Maintain comprehensive access logs and audit trails
- Utilize multi-factor authentication for record access

2 Data Preservation Protocols

- Implement immutable storage for critical corporate records
- Establish automated retention and deletion workflows
- Conduct quarterly system integrity and compliance audits

5. CONFIDENTIALITY AND ACCESS CONTROLS

1 Records shall be classified into the following access tiers:

- Public
- Internal
- Restricted
- Highly Confidential

2 Access to confidential records shall be strictly controlled through:

- Role-based access permissions
- Comprehensive user authentication
- Granular access logging
- Regular access privilege reviews

6. RECORD DISPOSITION

1 Record destruction must follow secure disposal protocols:

- Digital records: Cryptographic erasure
- Physical documents: Certified shredding
- Maintain comprehensive disposition logs
- Obtain written confirmation of destruction

7. COMPLIANCE AND ENFORCEMENT

1 Violations of this Policy may result in:

- Disciplinary action
- Potential termination of employment
- Legal prosecution for willful misconduct

2 Annual mandatory training on record management shall be conducted for all employees.

8. POLICY ADMINISTRATION

1 The Chief Legal Officer shall have primary responsibility for Policy interpretation and enforcement.

2 This Policy shall be reviewed annually and updated to reflect changing legal and technological landscapes.

9. DISCLAIMER

1 This Policy represents the current guidelines of Nexus Intelligent Systems, Inc. and is subject to modification at the Company's sole discretion.

Approved: January 22, 2024

—

Dr. Elena Rodriguez

Chief Executive Officer

Nexus Intelligent Systems, Inc.