ORGANIZATIONAL AND CORPORATE DOCUMENT 25

PREAMBLE AND RECITALS

THIS ORGANIZATIONAL AND CORPORATE DOCUMENT (this "Document") is made and entered into as of January 15, 2024 (the "Effective Date"), by and for NEXUS INDUSTRIAL INTELLIGENCE, INC., a Delaware corporation (the "Corporation"), having its principal place of business at 2500 Innovation Drive, Suite 400, Wilmington, Delaware 19801.

WHEREAS, the Corporation was incorporated under the laws of the State of Delaware on March 15, 2018, to develop and commercialize artificial intelligence and machine learning technologies for industrial applications, as evidenced by Certificate of Incorporation File No. 7654321;

WHEREAS, the Corporation has developed proprietary software solutions, including its flagship NexusCore™ Industrial AI Platform, combining computer vision, machine learning, and edge computing technologies for industrial process optimization, with applications across manufacturing, energy, and infrastructure sectors;

WHEREAS, the Corporation has secured substantial intellectual property rights, including U.S. Patents No. 11,123,456 and No. 11,234,567, covering fundamental aspects of its industrial artificial intelligence technologies;

WHEREAS, the Corporation maintains strategic partnerships with leading industrial enterprises and has deployed its technologies across multiple continents, serving Fortune 500 manufacturers and critical infrastructure operators;

WHEREAS, the Corporation desires to establish comprehensive organizational and operational frameworks to govern its continued development and deployment of industrial artificial intelligence solutions, ensuring compliance with applicable regulations and industry standards; and

WHEREAS, this Document shall serve to memorialize and govern the Corporation's organizational structure, intellectual property rights, operational protocols, and strategic initiatives in connection with its industrial technology business.

NOW, THEREFORE, the Corporation hereby adopts and establishes the following provisions:

1.0 DEFINITIONS AND INTERPRETATIONS

1.1 Defined Terms. For purposes of this Document, the following terms shall have the meanings specified below:

(a) "AI Technology" means the Corporation's artificial intelligence and machine learning algorithms, models, methodologies, and related technological implementations, including but not limited to computer vision systems, predictive analytics engines, process optimization algorithms, neural networks, deep learning frameworks, and automated decision-making systems.

(b) "Board" means the Board of Directors of the Corporation, including any duly appointed committees thereof and any successor governing body.

(c) "Confidential Information" means all non-public information relating to the Corporation's technology, products, business plans, customers, and operations, including but not limited to the AI Technology, Platform Technology, source code, algorithms, technical specifications, customer lists, pricing strategies, financial data, research and development activities, and trade secrets.

(d) "Customer Data" means any data received from, generated by, or pertaining to customers through their use of the Platform Technology, including but not limited to operational metrics, performance data, user behavior data, process parameters, and any derivative data sets created therefrom.

(e) "Industrial Applications" means the implementation and use of the Platform Technology in manufacturing, processing, and industrial operations environments, including automated production systems, quality control processes, supply chain optimization, predictive maintenance systems, and industrial Internet of Things (IoT) implementations.

(f) "Intellectual Property" means all patents, copyrights, trade secrets, trademarks, service marks, trade names, industrial designs, mask works, database rights, moral rights, and other intellectual property rights owned or controlled by the Corporation, whether registered or unregistered, and all applications and registrations thereof.

(g) "Platform Technology" means the NexusCore™ Industrial AI Platform and all associated software, systems, and technologies developed by the Corporation, including all updates, modifications, enhancements, derivatives, user interfaces, APIs, documentation, and related technical materials.

(h) "Authorized Users" means individuals or entities granted access rights to utilize the Platform Technology pursuant to valid licensing agreements.

(i) "Technical Documentation" means all manuals, specifications, protocols, guidelines, and other documentation relating to the implementation and operation of the Platform Technology.

1.2 Interpretation. In this Document:

(a) Section headings are for convenience only and shall not affect interpretation.

(b) Words importing the singular include the plural and vice versa.

(c) References to Sections are to Sections of this Document unless otherwise specified.

(d) The terms "including" and "includes" mean "including without limitation" and "includes without limitation" respectively.

(e) References to any statute, regulation, or standard include references to such statute, regulation, or standard as amended, supplemented, or replaced from time to time.

(f) Technical terms not specifically defined herein shall have the meanings commonly attributed to them in the industrial artificial intelligence and machine learning industry.

(g) References to time periods shall be calculated in calendar days unless otherwise specified.

(h) Any obligation not to do something includes an obligation not to permit or suffer that thing to be done.

2.0 CORPORATE ORGANIZATION

2.1 Corporate Status The Corporation is and shall remain a corporation duly organized and validly existing under the laws of the State of Delaware, with all requisite corporate power and authority to carry on its business as currently conducted. The Corporation shall maintain continuous good standing with the Delaware Secretary of State and all other jurisdictions where it conducts business operations. The Corporation shall promptly obtain and maintain all necessary licenses, permits, and authorizations required for its operations.

2.2 Authorized Capital Structure (a) The Corporation's authorized capital stock consists of: (i) 50,000,000 shares of Common Stock, par value $0.001 per share (ii) 10,000,000 shares of Preferred Stock, par value $0.001 per share

(b) Share Rights and Restrictions: (i) Common Stock shall carry one vote per share on all matters submitted to stockholder vote (ii) Preferred Stock may be issued in one or more series as determined by the Board (iii) The Board shall have authority to establish preferences, rights, and limitations of each Preferred Stock series (iv) All stock certificates shall bear appropriate legends regarding transfer restrictions

2.3 Board of Directors (a) Composition. The Board shall consist of not less than five (5) and not more than nine (9) directors, including: (i) The Chief Executive Officer (ii) At least one (1) director with artificial intelligence/machine learning expertise (iii) At least one (1) director with industrial manufacturing expertise

(b) Director Qualifications: (i) All directors must meet independence requirements under applicable securities laws (ii) Technology directors must possess minimum five years' relevant industry experience (iii) Directors shall maintain current knowledge of AI governance best practices (iv) No person under investigation for securities violations may serve as director

(c) Technology Oversight Committee. The Board shall maintain a Technology Oversight Committee responsible for: (i) Reviewing and approving major technology initiatives (ii) Monitoring AI governance and ethics (iii) Overseeing intellectual property strategy (iv) Evaluating cybersecurity measures and data protection protocols (v) Reviewing technology risk assessments quarterly (vi) Ensuring compliance with AI regulatory requirements

(d) Committee Operations: (i) The Committee shall meet at least quarterly (ii) Minutes shall document all technology and AI governance decisions (iii) Annual review of AI ethics guidelines required (iv) External technology advisors may be engaged as needed

2.4 Officers (a) Required Officers. The Corporation shall maintain the following officer positions: (i) Chief Executive Officer (ii) Chief Technology Officer (iii) Chief Financial Officer (iv) Chief AI Officer (v) Secretary

(b) Officer Qualifications: (i) CEO must have minimum ten years' executive experience (ii) CTO must possess advanced degree in computer science or related field (iii) CAO must demonstrate expertise in AI systems and ethics (iv) CFO must be certified public accountant or equivalent (v) All officers must pass background checks and security clearance

(c) Officer Duties. Each officer shall have such duties as prescribed by the Board and shall be responsible for ensuring compliance with this Document within their respective domains, including: (i) CEO: Strategic direction, overall management, and regulatory compliance (ii) CTO: Technology infrastructure, development roadmap, and innovation (iii) CAO: AI development, ethics compliance, and algorithmic governance (iv) CFO: Financial management, reporting, and internal controls (v) Secretary: Corporate records, governance, and regulatory filings

(d) Succession Planning: (i) Board shall maintain current succession plans for all officer positions (ii) Emergency succession protocols must be documented (iii) Annual review of succession readiness required (iv) Officer training and development programs maintained

2.5 Corporate Governance (a) The Corporation shall maintain comprehensive governance policies including: (i) Code of Ethics and Business Conduct (ii) AI Development and Usage Guidelines (iii) Intellectual Property Protection Protocols (iv) Data Privacy and Security Standards (v) Risk Management Framework (vi) Compliance Monitoring System

(b) Annual Review Requirements: (i) Board evaluation of governance effectiveness (ii) Independent audit of compliance systems (iii) Technology and AI risk assessment (iv) Officer performance evaluation (v) Stockholder communication procedures

3.0 INTELLECTUAL PROPERTY PROTECTION

3.1 Ownership of AI Technology (a) The Corporation shall retain exclusive ownership of all AI Technology, including: (i) All algorithms, models, and methodologies, including but not limited to machine learning architectures, neural network designs, and optimization techniques (ii) Training data and model parameters, encompassing both raw and processed datasets (iii) Implementation techniques and processes, including deployment frameworks and integration methods (iv) Associated documentation and materials, including technical specifications, architecture diagrams, and development logs (v) Any improvements, modifications, or derivative works thereof, regardless of creator or circumstances of creation

(b) Scope of AI Technology Definition (i) "AI Technology" shall encompass all computational systems, software, and methodologies that enable machine learning, pattern recognition, natural language processing, computer vision, and autonomous decision-making capabilities (ii) This definition extends to both current and future technological developments in the field of artificial intelligence (iii) Includes all supporting infrastructure, tools, and frameworks necessary for development and deployment

3.2 Patent and Trade Secret Protection (a) The Corporation shall maintain a comprehensive patent portfolio covering core AI Technology innovations, including: (i) Regular patent landscape analysis and strategic filing programs (ii) International patent protection in key markets and jurisdictions (iii) Defensive patent strategies to protect against infringement (iv) Regular portfolio review and maintenance procedures

(b) Trade Secret Protection. The Corporation shall: (i) Implement strict confidentiality protocols, including physical and digital security measures (ii) Maintain secure development environments with access controls and monitoring systems (iii) Require appropriate confidentiality agreements from all parties with access to proprietary information (iv) Control access to proprietary information through role-based authorization systems (v) Conduct regular security audits and vulnerability assessments (vi) Implement data classification and handling procedures (vii) Maintain incident response protocols for potential security breaches

3.3 Technology Licensing (a) Platform Technology shall be licensed to customers pursuant to written agreements that: (i) Preserve Corporation ownership of all IP rights and underlying technology (ii) Grant limited usage rights for Industrial Applications, clearly defining scope and restrictions (iii) Protect Confidential Information through comprehensive non-disclosure provisions (iv) Address Customer Data ownership and usage rights, including data privacy requirements (v) Establish clear terms for maintenance, support, and updates (vi) Define acceptable use policies and compliance requirements

(b) Licensing Framework Requirements (i) All licenses shall be non-exclusive unless explicitly authorized by executive management (ii) Territorial restrictions shall be clearly defined and enforced (iii) Sub-licensing shall be prohibited without express written permission (iv) Usage metrics and monitoring requirements shall be specified (v) Term and termination conditions shall be clearly outlined

3.4 IP Development Rights (a) All intellectual property developed by employees or contractors shall be owned by the Corporation, including: (i) Inventions, discoveries, and improvements related to AI Technology (ii) Software code, algorithms, and technical solutions (iii) Documentation, designs, and technical specifications (iv) Data models and training methodologies

(b) Employment and consulting agreements shall include: (i) Comprehensive IP assignment provisions (ii) Invention disclosure requirements (iii) Cooperation obligations for patent prosecution (iv) Post-employment confidentiality obligations (v) Non-compete and non-solicitation provisions where legally permissible

(c) The Corporation shall maintain rights to improvements and derivative works, including: (i) Modifications to existing AI Technology (ii) Extensions and enhancements of core functionality (iii) Integration solutions and implementation methods (iv) Customer-specific customizations and adaptations

3.5 IP Enforcement and Protection Measures (a) The Corporation shall maintain an active IP enforcement program, including: (i) Regular monitoring for potential infringement (ii) Investigation of unauthorized use or disclosure (iii) Enforcement action protocols and procedures (iv) Litigation strategy and resource allocation

(b) Protection Measures shall include: (i) Technical protection mechanisms and access controls (ii) Regular IP audits and compliance reviews (iii) Employee training and awareness programs (iv) Vendor and partner due diligence procedures (v) Documentation of IP ownership and chain of title

3.6 Third-Party IP Rights (a) The Corporation shall respect third-party IP rights through: (i) Comprehensive IP clearance procedures (ii) License compliance monitoring (iii) Open-source software usage policies (iv) Third-party technology integration protocols

(b) Risk Management Procedures (i) Regular IP portfolio risk assessment (ii) Indemnification and liability allocation (iii) Insurance coverage requirements (iv) Dispute resolution procedures

4.0 OPERATIONAL FRAMEWORK

4.1 Technology Development (a) Development Protocols (i) Standardized development methodologies shall be implemented across all project phases, including but not limited to agile frameworks, sprint planning, and iterative development cycles. All development teams must adhere to established protocols and maintain comprehensive documentation of methodology implementations. (ii) Code review and testing requirements shall encompass mandatory peer reviews, automated testing suites, and formal approval processes. Each code submission must undergo minimum three-tier review processes, including technical review, security assessment, and compliance verification. (iii) Documentation standards shall follow ISO/IEC/IEEE 29148:2018 guidelines for requirements engineering. All technical documentation must include system architecture diagrams, API specifications, data flow models, and detailed implementation guides. (iv) Security review procedures must align with NIST Cybersecurity Framework and include penetration testing, vulnerability assessments, and security architecture reviews at predetermined development milestones.

(b) Quality Control (i) Automated testing protocols shall incorporate unit testing, integration testing, and end-to-end testing methodologies. Test coverage metrics must maintain a minimum threshold of 85% across all production code. (ii) Performance benchmarking shall be conducted against established industry standards, with regular assessment of system latency, throughput, and resource utilization metrics. (iii) Validation procedures must include user acceptance testing, compliance verification, and performance validation under simulated production conditions. (iv) Release management processes shall follow ITIL v4 guidelines, including staged deployments, rollback procedures, and change management documentation.

4.2 Customer Deployment (a) Implementation Procedures (i) Customer readiness assessment shall evaluate technical infrastructure, personnel capabilities, and organizational change management requirements. Assessments must be completed minimum 30 days prior to deployment initiation. (ii) System integration planning must detail all technical dependencies, data migration requirements, and interface specifications. Integration plans shall include contingency measures and fallback procedures. (iii) Training requirements shall specify mandatory user training modules, certification requirements, and ongoing education programs. Training documentation must be maintained and updated with each major system release. (iv) Success metrics definition shall establish quantifiable performance indicators, including system utilization rates, error reduction metrics, and productivity improvements.

(b) Ongoing Support (i) Technical support protocols shall define service level agreements, escalation procedures, and response time requirements for various incident categories. (ii) Performance monitoring must include real-time system health checks, automated alerting mechanisms, and periodic performance reviews. (iii) Update procedures shall specify maintenance windows, version control requirements, and compatibility verification processes. (iv) Issue resolution framework must establish clear accountability, tracking mechanisms, and resolution timeframes for all support tickets.

4.3 Risk Management (a) Technology Risk Controls (i) Security protocols shall implement multi-layer security controls, including access management, encryption standards, and intrusion detection systems. All security measures must comply with ISO 27001 requirements. (ii) Backup procedures must ensure data redundancy through geographically distributed backup systems, with recovery point objectives (RPO) and recovery time objectives (RTO) clearly defined. (iii) Disaster recovery planning shall include detailed recovery procedures, communication protocols, and regular testing requirements. Plans must be reviewed and updated quarterly. (iv) Business continuity measures shall establish alternate processing capabilities, critical system failover procedures, and business impact analysis requirements.

(b) Compliance Framework (i) Regulatory compliance monitoring shall ensure adherence to applicable industry regulations, including but not limited to GDPR, CCPA, and sector-specific requirements. (ii) Industry standard adherence must be maintained through regular assessments against ISO 9001, ISO 27001, and relevant industry-specific standards. (iii) Audit procedures shall establish internal audit schedules, external audit requirements, and remediation tracking processes. (iv) Reporting requirements must include automated compliance reporting, incident reporting procedures, and regulatory disclosure obligations.

4.4 Governance Structure (a) Oversight Mechanisms (i) Establishment of a Technology Governance Committee with representation from key stakeholders. (ii) Regular review and approval of operational policies and procedures. (iii) Performance monitoring and accountability frameworks. (iv) Risk assessment and mitigation strategy reviews.

(b) Change Management (i) Formal change control procedures for all system modifications. (ii) Impact assessment requirements for proposed changes. (iii) Stakeholder communication protocols. (iv) Change implementation and verification procedures.

4.5 Continuous Improvement (a) Performance Optimization (i) Regular assessment of operational efficiency metrics. (ii) Implementation of process improvement initiatives. (iii) Technology stack optimization procedures. (iv) Resource utilization reviews.

(b) Knowledge Management (i) Documentation of lessons learned and best practices. (ii) Knowledge base maintenance requirements. (iii) Training program updates and revisions. (iv) Collaborative learning initiatives.

SIGNATURE AND EXECUTION

IN WITNESS WHEREOF, this Document has been executed as of the Effective Date first above written.

NEXUS INDUSTRIAL INTELLIGENCE, INC.

By: _______ Name: Dr. Sarah Chen Title: Chief Executive Officer

By: _______ Name: Michael Roberts Title: Chief Technology Officer

EXHIBITS

Exhibit A: Authorized Technology Stack Components Exhibit B: Standard Operating Procedures Exhibit C: Compliance Requirements Exhibit D: Risk Management Protocols

APPENDICES

Appendix 1: AI Governance Framework Appendix 2: Security Protocols Appendix 3: Quality Control Standards Appendix 4: Customer Success Metrics

[End of Document]